

No. 23A243

# In the Supreme Court of the United States

VIVEK H. MURTHY, U.S. SURGEON GENERAL, ET AL.,  
*Applicants,*

v.

STATE OF MISSOURI, ET AL., *Respondents.*

On Application for Stay of the Injunction Issued by the  
United States District Court for the Western District of Louisiana

## **SUPPLEMENTAL APPENDIX TO RESPONDENTS' RESPONSE TO PETITIONERS' THIRD SUPPLEMENTAL MEMORANDUM REGARDING APPLICATION FOR A STAY OF INJUNCTION**

**JEFFREY M. LANDRY**

*Attorney General of Louisiana*

**ELIZABETH B. MURRILL**

*Solicitor General*

*Counsel of Record*

**TRACY SHORT**

*Assistant Attorney General*

**D. JOHN SAUER**

*Special Ass't Attorney General*

Louisiana Dep't of Justice

1885 N. Third Street

Baton Rouge, Louisiana 70802

(225) 326-6766

*Counsel for State of Louisiana*

**ANDREW BAILEY**

*Attorney General of Missouri*

**JOSHUA M. DIVINE**

*Solicitor General*

**TODD A. SCOTT**

*Senior Counsel*

Office of the Attorney General

Supreme Court Building

207 W. High St.

P.O. Box 899

Jefferson City, Missouri 65102

Tel.: (573) 751-8870

Fax: (573) 751-0774

*Counsel for State of Missouri*

**JOHN J. VECCHIONE**

**JENIN YOUNES**

**ZHONETTE BROWN**

New Civil Liberties Alliance

1225 19th Street NW, Suite 450

Washington, DC 20036

(202) 918-6905

*Counsel for Respondents Dr.*

*Jayanta Bhattacharya, Dr.*

*Martin Kulldorff, Dr. Aaron*

*Kheriaty, and Jill Hines*

**JOHN C. BURNS**

Burns Law Firm

P.O. Box 191250

St. Louis, Missouri 63119

(314) 329-5040

*Counsel for Respondent Jim*

*Hoft*

## Index

<b>Description</b>	<b>Pages</b>
Deposition of Brian J. Scully (as publicly filed)	1a-456a
Exhibit 10 to Brian J. Scully Deposition	457a-518a
Exhibit 12 to Brian J. Scully Deposition	519a-613a
Exhibit 16 to Brian J. Scully Deposition	614a
Exhibit 17 to Brian J. Scully Deposition	615a-648a
Exhibit 18 to Brian J. Scully Deposition	649a-699a

BRIAN J. SCULLY 1/12/2023

1                   IN THE UNITED STATES DISTRICT COURT  
2                   FOR THE WESTERN DISTRICT OF LOUISIANA  
3                   MONROE DIVISION  
4   - - - - - x  
5   THE STATE OF MISSOURI           :  
6   et al.,                               :  
7                   Plaintiffs,           : No.  
8   v.                                    : 3:22-cv-01213-TAD-KDM  
9   JOSEPH R. BIDEN, JR.,           :  
10 et al.,                               :  
11                   Defendants.           :  
12 - - - - - x

13  
14                   Videotaped Deposition of BRIAN J. SCULLY  
15                   Thursday, January 12, 2023  
16                   9:06 a.m.

17  
18  
19  
20  
21   Job No.: 138046  
22   Pages 1 through 376  
23   Reported by: Cassandra E. Ellis, RPR

24  
25

1                   Deposition of BRIAN J. SCULLY, held  
2   pursuant to agreement, before Cassandra E. Ellis,  
3   Certified Shorthand Reporter -- Hawaii #475,  
4   Certified Court Reporter - Washington #3484,  
5   Certified Shorthand Reporter - California -  
6   #14448, Registered Professional Reporter #823848,  
7   Certified Realtime Reporter, Realtime Systems  
8   Administrator, and Notary Public of the District  
9   of Columbia.

10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25

1                                   A P P E A R A N C E S  
2           ON BEHALF OF PLAINTIFF:  
3                   D. JOHN SAUER, ESQUIRE  
4                   TODD SCOTT, ESQUIRE  
5                   KENT CAPPS, ESQUIRE  
6                   JOSH DIVINE, ESQUIRE  
7                   MISSOURI ATTORNEY GENERAL'S OFFICE  
8                   Supreme Court Building  
9                   221 W. High Street  
10                  P.O. Box 899  
11                  Jefferson City, Missouri 65101  
12                  (573) 751-8870  
13                  John.sauer@ago.mo.gov  
14                  Todd.scott@ago.mo.gov  
15  
16           ON BEHALF OF DEFENDANT:  
17                   JOSHUA E. GARDNER, ESQUIRE  
18                   INDRANEEL SUR, ESQUIRE  
19                   DEPARTMENT OF JUSTICE  
20                   1100 L Street, Northwest  
21                   Washington, D.C. 20530  
22                   (202) 514-3259  
23                   Joshua.e.gardner@usdoj.gov  
24                   Indraneel.sur@usdoj.gov  
25

1           A P P E A R A N C E S       C O N T I N U E D

2           O N B E H A L F O F D E F E N D A N T S :

3                   JESSICA SCHAU NELSON, ESQUIRE  
4                   Senior Counsel, Special  
5                   Litigation and Matters  
6                   Cybersecurity and Infrastructure  
7                   Security Agency  
8                   (202) 870-3578  
9                   Jessica.SchauNelson@cisa.dhs.gov

10  
11                   MATTHEW FLEISCHMAN, ESQUIRE  
12                   OFFICE OF THE GENERAL COUNSEL  
13                   U.S. DEPARTMENT OF HOMELAND SECURITY  
14                   (202) 746-8414  
15                   matthew.fleischman@hq.dhs.gov

16  
17  
18  
19           ALSO PRESENT:  
20           Joseph E. Ellis, Certified Legal Video Specialist

21  
22  
23  
24  
25

1	C O N T E N T S	
2	EXAMINATION OF BRIAN J. SCULLY	PAGE
3	By Mr. Sauer	11
4		
5		
6	E X H I B I T S	
7	(Attached to the Transcript)	
8	BRIAN J. SCULLY Deposition Exhibit	PAGE
9	Exhibit 1 EIP The Long Fuse:	69
10	Misinformation and the 2020 Election	
11	Exhibit 2 The Virality Project Memes	138
12	Magnets and Microchips Narrative	
13	Dynamics around COVID-19 VACCINES	
14	Exhibit 6 Audio Transcription Event:	368
15	Atlantic council: Lightning talk:	
16	Election Integrity Partnership	
17	JUNE 24, 2021	
18	Exhibit 7 Audio Transcription Event: CISA	369
19	Cyber Security Summit 2021: Responding	
20	to Mis, Dis, and mal-information	
21	OCTOBER 27, 2021	
22		
23		
24		
25		

1	E X H I B I T S	C O N T I N U E D	
2	(Attached to the Transcript)		
3	BRIAN J. SCULLY	Deposition Exhibit	PAGE
4	Exhibit 9	Assortment of Documents Bates	156
5	Stamped MOLA_DEFSPROD_00008353-355,		
6	9676-680, 8356-358, 10679-682,		
7	10603-605, 13661-663, 13511-517,		
8	7633-634, 8349-352, 13729-734,		
9	9603-605, 7583-587, 7574-576,		
10	10538-541, 7564-566, 8768-769,		
11	10512-516, 10523-526, 8496-498,		
12	8756-758, 8778-780, 10492-494		
13	Exhibit 10	Assortment of Documents	212
14	Bates Stamped MOLA_DEFSPROD_00008722-725,		
15	10449-453, 13603-609, 8739-741, 8696-700,		
16	10420-422, 8521-522, 8693-694, 8710-711,		
17	8695, 8663-667, 8660-662, 8689, 8679,		
18	8668-669, 8649-650, 8634, 8636-639,		
19	8631-632, 8628-630, 8640-643		
20	Exhibit 11	12/01/2020 E-mail(s) Bates	227
21	Stamped MOLA_DEFSPROD_00008600-604		
22	Exhibit 12	Defendants' Amended Combined	190
23	Objections and Responses to Plaintiffs'		
24	First Set of Expedited Preliminary-		
25	Injunction Related Interrogatories		



1	E X H I B I T S	C O N T I N U E D	
2	(Attached to the Transcript)		
3	BRIAN J. SCULLY	Deposition Exhibit	PAGE
4	Exhibit 13	Declaration of Yoel Roth dated	243
5	12/17/2020		
6	Exhibit 14	Excerpts of 11/29/2022 Elvis	249
7	Chan	Deposition	
8	Exhibit 15	04/14/2022 E-mail string Bates	252
9	Stamped	MOLA_DEFSPROD_00014552-553	
10	Exhibit 16	09/16/2020 E-mail Bates Stamped	252
11	MOLA_DEFSPROD_00013671		
12	Exhibit 17	Assortment of Documents Bates	252
13	Stamped	MOLA_DEFSPROD_00014551, 14545,	
14	14552-553, 15741-743, 14526-529,		
15	14545-547, 7598-600, 7654-659, 12076-079,		
16	13599, 13696-701		
17	Exhibit 18	Assortment of Documents Bates	277
18	Stamped	MOLA_DEFSPROD_00007669-670,	
19	10298-300, 8188-189, 10718, 9703,		
20	7484-487, 7552-554, 10564-565, 8519,		
21	10392-394, 10389-391, 8625-627,		
22	8623-627, 10410-412, 8595, 8586-587,		
23	8554-557, 12223-224, 12053-059		
24			
25			

1	E X H I B I T S C O N T I N U E D	
2	(Attached to the Transcript)	
3	BRIAN J. SCULLY Deposition Exhibit	PAGE
4	Exhibit 19 Elections Misinformation	363
5	Reporting Portal Bates Stamped	
6	MOLA_DEFSPROD_00012672	
7	Exhibit 21 CNN Politics Web Article CNN	364
8	Exclusive DHS rejects plan to protect	
9	Election officials from harassment as	
10	Midterms loom	
11	Exhibit 23 The Hill Web article Cyber	335
12	Agency beefing up disinformation,	
13	Misinformation team	
14	Exhibit 24 10/18/2022 CISA Mis, Dis,	365
15	Mal-information Team Announcement	
16	Exhibit 27 Cyberscoop Article CISA	301
17	Expands efforts to fight election	
18	Disinformation ahead of `challenging`	
19	2024 vote, dated 08/12/2022	
20	Exhibit 28 01/28/2022 E-mail Bates	306
21	Stamped MOLA_DEFSPROD_00011450-451	
22	Exhibit 29 Text Messages Bates Stamped	309
23	MOLA_DEFSPROD_00015749-751	
24		
25		

1	E X H I B I T S C O N T I N U E D	
2	(Attached to the Transcript)	
3	BRIAN J. SCULLY Deposition Exhibit	PAGE
4	Exhibit 30 The Intercept_ Truth Cops	319
5	Article Leaked Documents Outline	
6	DHS's Plan to Police Disinformation,	
7	Dated 10/31/2022	
8	Exhibit 31 OIG Report DHS Needs a	328
9	Unified Strategy to Counter	
10	Disinformation Campaigns, dated	
11	08/10/2022	
12	Exhibit 46 CISA Draft Report to the CISA	352
13	Director, dated 06/22/2022 Bates	
14	Stamped MOLA_DEFSPROD_00015459-463	
15	Exhibit 49 The Breakdown Article Brian	345
16	Scully on government response to	
17	Disinformation, dated 06/18/2020	
18	Exhibit 52 02/17/2022 E-mail string Bates	349
19	Stamped MOLA_DEFSPROD_00015736-737	
20	Exhibit 59 02/11/2022 E-mail Bates Stamped	359
21	MOLA_DEFSPROD_00011414-415	
22	Exhibit 61 NRMC Election Security Initiative	13
23	Organizational Chart - August 2022	
24	Exhibit 62 LinkedIn Profile of Jack Cable	194
25	Public Interest Technologist	

1 P R O C E E D I N G S

2 THE VIDEOGRAPHER: We are on the  
3 record. Today's date is January 12th, 2023, and  
4 the time is now 9:06 a.m. This is the video  
5 recorded deposition of Brian Scully in the  
6 matter of the State of Missouri, et al.,  
7 plaintiff, versus Joseph R. Biden, Junior, et  
8 al., defendants, Case Number  
9 3:22-CV-01213-TAD-KDM in the United States  
10 District Court for the Western District of  
11 Louisiana, Monroe Division.

12 This deposition is being held via  
13 Zoom.

14 The reporter's name is Cassandra  
15 Ellis. My name is Robyn Ellis. I'm the legal  
16 videographer. We are with Lexitas Legal.

17 Would the attorneys present please  
18 introduce themselves and parties they represent.

19 MR. SAUER: John Sauer, from the  
20 Missouri Attorney General's Office, on behalf of  
21 the plaintiffs. And I'm joined by my colleague,  
22 Todd Scott, who's in the room with the witness,  
23 also of the Missouri Attorney General's Office.

24 MR. GARDNER: And this is Josh  
25 Gardner, with the United States Department of

1 Justice, on behalf of the defendants, and  
2 witness does reserve the right to read and sign.

3 With me today is Jessica Nelson,  
4 with CISA. Matt Fleischman, with the Department  
5 of Homeland Security and Indraneel Sur, with my  
6 office, the Department of Justice. We all  
7 represent the defendants.

8 THE VIDEOGRAPHER: Would the court  
9 reporter please swear in the witness.

10 (Witness sworn)

11 THE VIDEOGRAPHER: You may proceed.

12 BRIAN J. SCULLY

13 having been duly sworn, testified as follows:

14 EXAMINATION

15 BY MR. SAUER:

16 Q. Mr. Scully, could you please state  
17 your full name for the record?

18 A. Sure. Brian Joseph Scully.

19 Q. How long -- or what is your current  
20 job title?

21 A. Brand P for the MDM branch, at the  
22 National Risk Management Center, which is part  
23 of the Department of Homeland Security.

24 Q. How long have you had that  
25 particular job?

1 A. Almost -- almost four years, I  
2 started in January 2019.

3 Q. What did you do before that?

4 A. I was a deputy for the countering  
5 and foreign influence task force, starting in  
6 April-ish, April/May 2018.

7 Q. And what was your -- what was your  
8 job before that one?

9 A. I was a director for policy and  
10 strategy in the Office of Infrastructure  
11 Protection.

12 Q. Have you ever given a deposition  
13 before?

14 A. I have not.

15 Q. So this is your first one?

16 A. This is my first deposition.

17 Q. Can I just go over some common  
18 ground rules with you?

19 First of all, obviously what you  
20 and I say is being transcribed by the court  
21 reporter, so can we make an effort not to talk  
22 too fast?

23 A. Yep.

24 Q. And could you give -- I saw you nod  
25 your head there, and then you said yes. Could

1       you try and give a verbal answer to my  
2       questions, you know, don't rely on uh-huh or  
3       uhn-uhn or head shaking as we go forward today.

4             A.    Yes, I can do that.

5             Q.    Can we make an effort not to  
6       interrupt each other, because that results in a  
7       kind of confused transcript.

8             A.    Of course.

9             Q.    Okay. And then can you make an  
10      effort to listen carefully to the question that  
11      I'm asking you, and respond to the question that  
12      I ask, instead of discussing some other  
13      tangential topic as the day goes forward?

14            A.    Of course.

15            Q.    And you understand --

16            A.    Yes.

17            Q.    You understand that at the end of  
18      the day, if your attorney wants to ask you some  
19      follow-up questions he may have the opportunity  
20      to do that.

21                    But when -- as I ask questions, I  
22      would ask you to focus on the questions I'm  
23      asking you, and respond to those; is that fair?

24            A.    That's fair.

25                    (Exhibit No. 61 was marked for

1 identification.)

2 BY MR. SAUER:

3 Q. Let me start by showing you an  
4 exhibit, and I apologize, this exhibit is out of  
5 numerical order already, so I'm e-mailing it to  
6 your counsel right now. It's pre-marked Exhibit  
7 61, but it will be the first exhibit we look at  
8 today.

9 And I'm going to pull it up on the  
10 screen share. Can you see that screen share?  
11 I'm going to zoom in a little bit.

12 MR. GARDNER: Hey, John, it hasn't  
13 come through yet, the e-mail, so it's just --  
14 unfortunately, that's kind of far away, it's a  
15 little challenging to see, but as soon as we get  
16 your e-mail we'll pull it up.

17 MR. SAUER: You said you can't see  
18 what's on the screen share if I zoom in?

19 MR. GARDNER: As you make it larger  
20 it's easier, but I don't want to speak for what  
21 the witness can and can't see.

22 THE WITNESS: Yeah, I can see it.

23 BY MR. SAUER:

24 Q. Okay. I'm happy to wait until it  
25 arrives on the e-mail. I just want to make



1       sure, because I think the day's going to go more  
2       smoothly, if I can direct your attention to  
3       stuff on the screen share.

4                       So you can see the screen share,  
5       sir?

6               A.    Yes, I can.

7               Q.    Okay. Just looking at the top of  
8       this document, do you recognize it as an org  
9       chart for August 2022, of a subdivision of CISA?

10              A.    Yes.

11              Q.    And what -- what -- are you  
12       familiar with this org chart?

13              A.    Somewhat familiar with it, yes.

14              Q.    I just want to direct your  
15       attention over here on the right side of the  
16       page, you see here where it lists you as the  
17       chief of the mis, dis and mal-information team?

18              A.    Okay.

19              Q.    Is that your job title?

20              A.    Yes.

21              Q.    Yeah, what, exactly -- generally  
22       speaking, what do you do as the chief of the  
23       mis, dis and mal-information team for CISA, the  
24       Cyber Security and Infrastructure Security  
25       Agency?

1           A.     So I -- obviously I manage the  
2     team, as a team lead. So I manage the staff,  
3     set priority, things like that.

4           The purpose of the team is to build  
5     national resilience to MDM, targeting critical  
6     infrastructure.

7           **Q.     Generally speaking, what kind of**  
8     **activities are involved in building resilience**  
9     **to critical infrastructure -- or sorry --**

10          A.     We felt -- sure.

11          So principally what we do is  
12     develop products for public awareness and  
13     education or products for key stakeholders to  
14     help them understand how MDM works and steps  
15     they can take to mitigate the risks.

16          **Q.     Do you do anything else, besides**  
17     **developing products?**

18          A.     We engage with different  
19     stakeholders, civil society groups, obviously  
20     other federal partners, private sector  
21     organizations, and then we -- we do some  
22     analysis of open source reporting, and we do --  
23     obviously, you know, in 2020 we did some  
24     switchboard work on behalf of election  
25     officials.

1 Q. Switchboard work, what does that  
2 mean?

3 A. It was essentially an audit  
4 official to identify something on social media  
5 they deemed to be disinformation aimed at their  
6 jurisdiction. They could forward that to CISA  
7 and CISA would share that with the appropriate  
8 social media companies.

9 Q. And what was the purpose of sharing  
10 it with social media companies?

11 A. Mostly for informational awareness  
12 purposes, just to make sure that the social  
13 media companies were aware of potential  
14 disinformation.

15 Q. Was there an understanding that if  
16 the social media platforms were aware of  
17 disinformation that they might apply their  
18 content moderation policies to it?

19 A. Yes. So the idea was that they  
20 would make decision on the content that was  
21 forwarded to them based on their policies.

22 Q. Whereas, if it hadn't been brought  
23 to their attention then they obviously wouldn't  
24 have moderated it as content; correct?

25 A. Yeah, I suppose that's true, as far

1 as I'm aware of it.

2 Q. Directing your attention to the org  
3 chart again, can you -- I would sort of walk  
4 through the people here on your team and ask  
5 you, kind of who they are and what they do, so  
6 starting on the right column, I see Lauren  
7 Protentis on as the engagements lead; who is she  
8 and what does she do for your team?

9 A. So she was -- she's a -- she's the  
10 engagements lead. So her job was engaging with  
11 key stakeholders, interagency partners, private  
12 sector partners, essentially a majority of  
13 our outreach and engagement efforts, she managed  
14 those.

15 Q. Outreach and engagement to key  
16 stakeholders, does that include social media  
17 platforms?

18 A. It did, yeah.

19 Q. When you say: "It did," does she  
20 still do this or does she no longer communicate  
21 with social media platforms?

22 A. Well, she's on the -- she's been on  
23 maternity leave since September, so she's --  
24 she's not currently doing it, when she returns  
25 to CISA that would be her role.

1 Q. Who's doing it while she's gone?

2 A. And she -- I'm sorry, could you  
3 repeat that?

4 Q. Who's -- who's playing that role in  
5 her absence?

6 A. I am.

7 Q. Okay. And so for the past, I  
8 guess, three or four months you've served as  
9 essentially the active engagements lead for the  
10 MDM team?

11 A. Correct.

12 Q. And that goes back, I think you  
13 said, to September of 2022; is that right?

14 A. Correct.

15 Q. When do you expect Ms. Protentis to  
16 return?

17 A. Her maternity leave ends in a  
18 couple of weeks, I believe the 23rd, potentially  
19 being gone on a detail assignment, so probably  
20 January 2024.

21 Q. Oh, so you don't expect her back  
22 for another year, because of the detail?

23 A. Correct.

24 Q. Is the detail in -- relate to  
25 anything having to do with mis, dis or

1 mal-information?

2 A. I believe that will be part of her  
3 portfolio on the detail, yeah.

4 Q. Where is she going, if I may ask?

5 A. The National Security Council.

6 Q. And in her absence, you're serving  
7 as the kind of person who directly communicates  
8 with social media platforms, among other  
9 stakeholders?

10 A. Correct.

11 Q. I should mention, you used the  
12 shorthand earlier, MDM, and I assume it will  
13 come up again today. When you use that, you're  
14 referring to mis, dis and mal-information;  
15 right?

16 A. Correct.

17 Q. I think sometimes CISA refers to MD  
18 to refer to mis and disinformation; is that  
19 right?

20 A. I'm not sure I've ever seen us use  
21 MD, but that would be proactive in the context,  
22 yeah.

23 Q. Turning your attention back to the  
24 period from September of 2022 to the present,  
25 what sorts of communications have you had with

1       **social media platforms in Ms. Protentis's stead?**

2               A.     Two -- I would say two general  
3       types of communications, one, we did regular  
4       sync meetings between government and industry,  
5       so federal partners and different social media  
6       platforms. So it's just a coordinated meeting.

7               Facebook was the industry lead, so  
8       I would have coordination calls with them prior  
9       to the meetings, just to set the agenda for the  
10      meetings, so that was one.

11              And then two, if a platform was  
12      putting out a public statement -- or not public  
13      statement -- public report on policies or  
14      activities, we would often get a briefing on  
15      that or at least get an awareness that it was  
16      going out.

17              Those are the two main types of  
18      communications.

19              **Q.    Did you -- were you involved in the**  
20      **last -- in the period since September 2022, and**  
21      **have you been involved in flagging any**  
22      **misinformation or disinformation issues for**  
23      **social media platforms?**

24              A.     No, not that we recall. We didn't  
25      do switchboarding in 2022.

1 Q. So when was that decision made not  
2 to do switchboarding in 2022?

3 A. I believe it was back in April that  
4 that decision was made?

5 Q. Who made that decision?

6 A. April 2022.

7 Q. Was that early or late April, do  
8 you know?

9 A. I don't. I don't recall.

10 Q. Who made that decision?

11 A. I -- I heard about it through Geoff  
12 Hale, who is -- is a senior org chart would be  
13 my supervisor. I believe he received that  
14 guidance from the director, Director Easterly.

15 Q. So in -- some time around -- was  
16 this late April?

17 A. Honestly, I don't recall. It's  
18 even possible it was in May by the time -- my  
19 memory's a little foggy on it -- but the  
20 earliest it was is probably mid April.

21 Q. Do you know --

22 A. And it could have gone any time  
23 into early May.

24 Q. So the earliest would have been  
25 late April, but possibly early May is when that



1           **decision was made; correct?**

2                           MR. GARDNER:  Objection.

3  BY MR. SAUER:

4                           **Q.  Correct?**

5                           MR. GARDNER:  Sorry.  Objection,  
6  mischaracterizes the witness's previous  
7  testimony.

8                           A.  Yeah, the earliest would have been  
9  mid April --

10                          **Q.  The earliest would have been mid**  
11 **April?**

12                          A.  -- probably.

13                          **Q.  Okay.  And then possibly beginning**  
14 **of May?**

15                          A.  Yeah.

16                          **Q.  And you said -- you called this**  
17 **switchboarding.**

18                          A.  Mm-hmm.

19                          **Q.  Switchboarding refers to routing**  
20 **particular disinformation concerns to social**  
21 **media platforms so they can evaluate them under**  
22 **the content modulation -- modulation policies;**  
23 **correct?**

24                          A.  So switchboarding is CISA's role in  
25  forwarding reporting received from election

1 officials, state/local election officials, to  
2 social media platforms.

3 **Q. CISA forwarded disinformation**  
4 **concerns from many other sources, besides state**  
5 **and local election officials, to social media**  
6 **platforms?**

7 A. I don't believe so, not that I  
8 recall.

9 **Q. Turning back to the two kinds of**  
10 **interactions you had with social media**  
11 **platforms, the last months since September of**  
12 **2022, the first one you mentioned was, I**  
13 **believe, a sync meeting between social media**  
14 **platforms and the US government; correct?**

15 A. Correct.

16 **Q. How often did those occur?**

17 A. They started as monthly, until, I  
18 think, October. And then we did a couple of  
19 biweekly, I believe two biweekly meetings --

20 **Q. What was the purpose of the --**

21 A. -- prior to the election.

22 **Q. What was the purpose of these**  
23 **meetings?**

24 A. Generally speaking, from a CISA  
25 perspective, we would -- we would provide kind

1 of -- we would try to educate the platforms on  
2 how elections actually function, how they're  
3 administered, potential threats to the election  
4 administration, things like that.

5 So CISA's -- you know, has some  
6 expertise in the election security space. So  
7 our role in the meetings was generally to  
8 provide kind of expertise on how elections  
9 actually work to the platforms.

10 **Q. And you said that was your role.**

11 **Were there other federal agencies**  
12 **involved in these meetings?**

13 A. There were, and -- and that role  
14 was generally Geoff Hale. My role in the  
15 meetings was generally to just oversee them,  
16 facilitate the meetings.

17 Other agencies would provide  
18 high-level reviews or strategic intelligence  
19 briefs, if they had any -- anything to share  
20 that was unclassified.

21 **Q. What sorts of -- first of all, what**  
22 **agencies participated?**

23 A. DOJ, FBI, ODNI, and then DHS.

24 **Q. When you say DHS, was that just**  
25 **CISA, you and Geoff Hale, or were there other**

1           **components of DHS involved?**

2                   A.     The Office of Intelligence and  
3           Analysis of DHS also participated.

4                   **Q.     And that's called IA; is that**  
5           **correct?**

6                   A.     Correct.

7                   **Q.     And what was -- what did they say**  
8           **at these meetings, I&A?**

9                   A.     If they put out unclassified  
10          reporting, under their normal mandate, they  
11          would just talk about the reporting that they --  
12          that they published, that was related to  
13          election security.

14                  **Q.     What kind of reporting did they do,**  
15          **is it about foreign influence or is it about**  
16          **domestic threats, what kind of reporting do they**  
17          **do?**

18                  A.     I'm not a hundred percent certain  
19          of their -- their mission of authority. I  
20          believe and recall what they talked about, they  
21          certainly talked about foreign threats. I'm not  
22          sure -- they may have also talked a little bit  
23          about domestic terrorism threats, but I think  
24          that -- but I'm not 100 percent certain.

25                  **Q.     Like what sorts of things are they**

1       saying to social media platforms, are they  
2       saying, hey, you're going to see this kind of  
3       content popping up on Facebook and Twitter and  
4       so forth, and, you know, therefore, we want you  
5       to be alert to it, what kind of -- what's the  
6       purpose of giving them these briefings?

7               A.     So generally speaking, it's hard  
8       for me to speak directly to the I&A reporting  
9       because, you know, I don't recall all the  
10      details of it, but generally speaking, it was  
11      more strategic-level. So high-level things that  
12      they might be seeing, actors that might be  
13      interested in undermining confidence in the  
14      elections.

15               If they were seeing potential  
16      domestic terrorism type threats, those sorts of  
17      things, generally speaking, at least as long as  
18      I recall, there was never any discussion of  
19      specific content.

20               Q.     Did they identify specific domestic  
21      actors who they believed might try to undermine  
22      confidence in election outcomes through social  
23      media?

24               A.     Not that I recall.

25               Q.     Let me ask this: Who, on the

1       **government side of these meetings, who**  
2       **participates on behalf of -- who participated on**  
3       **behalf of CISA?**

4               A.     Geoff Hale and myself were the  
5       primaries, and then you might have others who  
6       were in listen-only mode. So Kim Wyman, for  
7       example, would sometimes be in listen-only mode.  
8       Allison Snell would sometimes be essentially the  
9       deputy or, slash, chief of staff of the --  
10      underneath Geoff, she would sometimes be in  
11      listen-only mode. And then obviously when  
12      Lauren was pre-maternity leave she would also be  
13      on.

14              **Q.     And then for I&A, who was on these**  
15      **meetings?**

16              A.     In 2022, I believe Luke Beckman was  
17      the lead. And then they would, depending on,  
18      you know, what product they were briefing, they  
19      would bring an analyst on, so those would  
20      change.

21              **Q.     Do you remember any other human**  
22      **beings, besides Luke Beckman, from I&A, who**  
23      **participated in these meetings in the period of**  
24      **time we're talking about, from September 2022 to**  
25      **the present?**

1           A.    I don't know. Like I -- Luke was  
2           the kind of principal lead, and who I coordinate  
3           with, I don't recall the analysts' names that  
4           they might have on there now.

5           **Q.    What's his title?**

6           A.    Honestly, I don't know. I believe  
7           he's in the cyber mission center, but they are  
8           odd up there, so I'm not entirely sure what his  
9           title was, sorry.

10          **Q.    You mentioned FBI had**  
11          **representatives at these meetings; is that**  
12          **right?**

13          A.    Correct.

14          **Q.    Who from FBI participated in these**  
15          **meetings?**

16          A.    I recall Laura Dehmlow, at least  
17          one, and I forget who -- who the other folks  
18          were.

19          **Q.    How many FBI people?**

20          A.    Generally, there would be one,  
21          maybe two.

22          **Q.    How about Elvis Chan, was he on**  
23          **these meetings?**

24          A.    Oh, good reminder. Thank you.  
25                Yes, he would be on some of them,

1 as well. I forgot about Elvis.

2 Q. Do you remember anyone else,  
3 besides him?

4 A. There would be, again, periodically  
5 other people would be on from different parts of  
6 FBI, but again, Laura was usually who we  
7 coordinated through, and I don't really  
8 remember -- I don't really remember the other  
9 names, sorry.

10 Q. When you say Laura, that's Laura  
11 Dehmlow is who you coordinated through?

12 A. Correct.

13 Q. When you say: You coordinated  
14 through them, what kind of coordination did CISA  
15 do with FBI as it pertained to these meetings?

16 A. Yeah, so basically coordinating  
17 time and the logistics of the meeting, and then  
18 two, if they had any particular agenda items  
19 they wanted to raise, you know, when we were  
20 putting together the agenda, I would just check  
21 with them to see if they had any -- any  
22 particular agenda items they wanted to raise.

23 Q. What sort of agenda items did they  
24 raise?

25 A. I don't believe in the time I was



1 working, you know, in the timeframe we're  
2 talking about, I don't believe that they raised  
3 any.

4 Q. Do you have -- how about before  
5 that, when Ms. Protentis was still handling the  
6 meetings?

7 A. Not -- not that I recall. Yeah, I  
8 don't -- I don't -- I don't recall, in  
9 particular, yeah, sorry.

10 Q. And I take it these meetings, we've  
11 been talking about them in the period from last  
12 September until now, but they're actually going  
13 on intermittently, at least, for years; right?

14 A. Yeah, so the first meeting we had  
15 with -- between federal and -- and industry was  
16 in 2018.

17 Q. Yeah, we're talking -- we're now  
18 kind of four years in, and then in terms of  
19 their frequency I take it they -- they --  
20 they're less frequent when you're further away  
21 from election, and they become monthly as the  
22 election gets closer, and then they become  
23 weekly or biweekly, you know, within the last  
24 month or so before an election; is that right?

25 A. I would say 2018, 2019 they were

1 very infrequent, so we maybe did them quarterly  
2 or less. And then sometime in 2020 we started  
3 monthly. And then, like you said, as we got  
4 closer to the election they would pick up. And  
5 then after the election they would -- we would  
6 spread them back out again.

7 But 2018 and 2019 was different  
8 than 2020 and beyond.

9 Q. And is there a plan to have these  
10 meetings continue in 2023?

11 A. Not currently.

12 Q. So you don't know -- you don't know  
13 whether there's going to be quarterly meetings  
14 or anything like that in 2023?

15 A. Correct.

16 Q. Who from DOJ was at these meetings?

17 A. Rodney Patton -- Patton.

18 Q. Anyone else?

19 A. No, not that I recall.

20 Q. How do you spell his last name?

21 A. I believe it's P-a-t-t-o-n.

22 Q. Like the general?

23 A. Yes.

24 Q. What -- what is his title at DOJ?

25 A. I don't know what his title is, but

1 I believe he's in the national security  
2 division.

3 Q. Was national security division of  
4 DOJ participating in these meetings leading up  
5 to the 2020 election?

6 A. Yes.

7 Q. Who from NSD participated in those  
8 meetings?

9 A. I believe it was Rodney, back then,  
10 as well.

11 Q. Do you remember anyone else?

12 A. Adam Hickey may have jumped on a  
13 couple.

14 Q. Is he also from the national  
15 security division of DOJ?

16 A. I believe so, yeah.

17 Q. Is that H-i-c-k-e-y?

18 A. Yes.

19 Q. What, if anything, did DOJ say in  
20 these meetings?

21 A. Generally speaking, they didn't say  
22 anything. Yeah, I don't recall in 2022 or even  
23 back in 2020 that they were -- were particularly  
24 active in the meetings.

25 Q. Do you remember anyone from DOJ

1           **saying anything at any point?**

2                   A.    I mean, I'm -- I'm sure they did,  
3           but I don't recall.

4                   **Q.    Do you remember anyone from DOJ**  
5           **ever, you know, putting an agenda items on the**  
6           **calendar for these meetings?**

7                   A.    I don't, no.

8                   **Q.    How about ODNI, the Office of the**  
9           **Director of National Intelligence, what human**  
10           **being from there participated in these meetings**  
11           **in 2022?**

12                   A.    Is it okay if I ask my attorneys a  
13           quick question?

14                   **Q.    The question --**

15                   MR. GARDNER:  Is it about a  
16           privilege?

17                   THE WITNESS:  Yeah.

18                   MR. GARDNER:  Yeah, John, if you  
19           want him to answer that question we'll need to  
20           recess quickly so he can consult with counsel  
21           about these issues of privilege.

22                   MR. SAUER:  Let's go off the  
23           record.

24                   THE VIDEOGRAPHER:  The time is now  
25           9:32.  We're off the record.

1 (Recess.)

2 THE VIDEOGRAPHER: The time is now  
3 9:34. We're back on the record.

4 MR. GARDNER: And counsel, I will  
5 instruct the witness not to answer that question  
6 on the basis of the National Security Act, that  
7 information is extraordinarily protected.

8 MR. SAUER: Before we proceed, I --  
9 I'm announcing, for the record, that Mr. Kent  
10 Capps, from the Missouri Attorney General's  
11 Office joined the call on behalf of plaintiffs  
12 in the last break.

13 BY MR. SAUER:

14 Q. Was there anyone -- how many  
15 individuals from ODNI participated in these  
16 meetings in 2022?

17 A. I believe there were two to three.

18 Q. Without telling me who they are, do  
19 you remember who they are?

20 A. I remember one's name and one's  
21 position, the second one's position.

22 Q. How about 2020, how many --

23 A. Again, it was -- it was three or  
24 four.

25 Q. Do you remember who they were?

1 A. I remember the lead person's name.

2 Q. Did people from ODNI speak in these  
3 meetings during 2022?

4 A. Yes.

5 Q. What did they say?

6 A. Again, generally speaking, if they  
7 had some strategic intelligence, unclassified,  
8 strategic intelligence reporting, they might  
9 share a quick summary of that. It was fairly  
10 limited in the timeframe from September  
11 through -- through the election, though.

12 Q. Were you in the meetings prior to  
13 September of 2022, when Ms. Protentis was still  
14 at your team?

15 A. I joined several of them over the  
16 summer, a couple -- couple of them over the  
17 summer, prior to her departure. And that was  
18 just the meetings, themselves, not necessarily  
19 the coordination meetings prior to the actual  
20 sync meetings.

21 Q. So the coordination meeting, is  
22 that a bilateral meeting that happens between  
23 CISA and Facebook?

24 A. Yes, CISA and Facebook, and then we  
25 would do CISA with the interagency. We would

1 do -- federal interagency partners would do a  
2 coordination meeting.

3 Q. That would be separate from the  
4 meeting with Facebook?

5 A. Correct.

6 Q. Would there be two preparatory  
7 meetings, one between CISA --

8 A. Generally, yes.

9 Q. One between --

10 A. Sorry.

11 Q. -- CISA and Facebook, and one  
12 between CISA and other federal agencies?

13 A. Yes, that is correct.

14 Q. Turning back to what ODNI said at  
15 these meetings in 2022, what do you remember,  
16 more specifically, that they said? Did they  
17 ever raise a specific threat advisory?

18 A. Not that I recall. I -- again,  
19 generally speaking, it was -- it was -- I don't  
20 recall specifics, so I'll just say that upfront.

21 And generally speaking, it was --  
22 it was higher level, kind of strategic of what a  
23 threat actor may be considering or thinking  
24 about.

25 Q. And do they identify specific

1       **threat actors?**

2               A.     Potential state actors, yeah, so  
3     other countries.

4               **Q.     How about domestic actors?**

5               A.     No, not that I recall.

6               **Q.     Did anyone on the US government**  
7     **side, in these meetings, identify domestic**  
8     **actors in the lead-up to the 2022 election?**

9               A.     They -- they may identify domestic  
10    actors, generally, but not -- to my  
11    recollection, there's no mention of specific  
12    actors, individuals, or groups that I recall.

13              **Q.     What social media platforms**  
14    **participated in these meetings?**

15              A.     So obviously Facebook, Twitter,  
16    Microsoft, Google, Reddit generally  
17    participated, I believe sometimes LinkedIn would  
18    join. They're a subsidiary of Microsoft, so  
19    generally we worked through Microsoft. Those  
20    are the ones that I recall.

21                     I believe there are others, as  
22    well, at different times, that maybe  
23    participated in a meeting or two.

24                     But from September 2022 to the  
25    election, I think it was principally the five I



1 mentioned.

2 **Q. How about Wiki Media Foundation?**

3 A. I know they participated in some, I  
4 don't know how frequently, and if it -- I don't  
5 recall them participating from September on, but  
6 it's possible.

7 **Q. Were concerns about misinformation**  
8 **and disinformation on social media platforms**  
9 **discussed in these meetings in the 2022**  
10 **timeframe?**

11 A. Yes.

12 **Q. What -- what was -- what was said**  
13 **about those concerns and by whom?**

14 A. Again, it was a more general  
15 approach. So from a CISA MDM team perspective,  
16 if we were developing any products we would  
17 discuss those. We didn't -- we released, I  
18 believe, two sets of products in that timeframe.

19 And in others, if there was the  
20 intelligence community, if they're reporting  
21 included foreign actors who were potentially  
22 going to use information operations, they might  
23 mention that in their briefings. But I don't  
24 remember specific, you know, what the specifics  
25 of every kind of mention were.

1 Q. But you --

2 A. And then the platforms -- sorry, to  
3 give you both sides, that was just the  
4 government side -- the platforms, they might  
5 share some high-level trend information from  
6 public reporting that they put out. So a lot of  
7 the platforms do their own regular reports on  
8 what they're seeing on their platforms and what  
9 they're -- what actions they're taking. And so  
10 the platforms, themselves, would share that type  
11 of information.

12 Q. So they would report to the  
13 government on what sorts of mis and  
14 disinformation they were seeing on their  
15 platforms and what content moderation actions  
16 they were taking with respect to it?

17 A. So they would share essentially  
18 what they were getting ready to make public or  
19 what they had already made public. So they  
20 would share kind of what they're seeing in their  
21 public reports, and then potentially provide  
22 some additional context around that.

23 So as I mentioned, most of the  
24 platforms would put out regular public reporting  
25 on what they were doing and what actions they

1 were taking. And so they would share that, and  
2 if the government had questions or was looking  
3 for additional context they would often talk  
4 about that, they would generally talk about any  
5 new tactics that they were seeing.

6 Most of what they -- my  
7 recollections for the time period we're talking  
8 about here, from September 2022 to the election  
9 in 2022, I recall most of it was foreign based.

10 But, you know, when we -- often  
11 what you see overseas essentially makes its way  
12 to the United States. So they would share kind  
13 of trends and tactics that they were seeing, but  
14 again, it was all based on public reporting that  
15 they put out.

16 **Q. And you say that this -- all these**  
17 **things that they're doing all relate to**  
18 **misinformation and disinformation on the**  
19 **platforms; correct?**

20 A. They don't call it misinformation  
21 or disinformation, generally, on the platforms.  
22 They generally define it as coordinated  
23 inauthentic behavior.

24 So they -- so -- so that's how they  
25 would describe it. They wouldn't normally kind

1 of say misinformation or disinformation. And  
2 they would each kind of define coordinated and  
3 inauthentic behavior differently.

4 I don't -- so I don't know that  
5 they would agree. I don't want to speak for the  
6 platforms, obviously. I don't know if they  
7 would agree that they were framing it as  
8 misinformation or disinformation.

9 **Q. From the CISA MDM teams**  
10 **perspective, is coordinated inauthentic behavior**  
11 **typically a kind of mis and disinformation?**

12 A. It could lead to mis or  
13 disinformation, for sure, yeah. But it's not  
14 always mis or disinformation.

15 **Q. So the coordinated and inauthentic**  
16 **behavior may be a source of mis or**  
17 **disinformation of particular concern?**

18 A. It could be, yeah. It could be an  
19 indicator.

20 **Q. Let me ask this: Turning back to**  
21 **the org chart, that should be on the screen,**  
22 **below Ms. Protentis, is Chad Josiah, who's**  
23 **described as the resilience lead. What is his**  
24 **role on your team?**

25 A. So he manages the production of our

1 products. So, you know, for putting out a fact  
2 sheet or, for example, we have several graphic  
3 novels that we've developed, he would work and  
4 manage that process to get the products out, so  
5 the review process, the drafting process, things  
6 like that.

7 **Q. These products you're referring to,**  
8 **I take it those are written, publicly available**  
9 **bulletins or other written work products**  
10 **discussing disinformation and misinformation; is**  
11 **that right?**

12 A. Correct. All of our product are  
13 available on our website.

14 **Q. Below him is Alex Zaheer, analyst;**  
15 **what does he do?**

16 A. He's a more junior analyst. He  
17 supports essentially across our three lines of  
18 work. So he helps Chad on some, he helps Warren  
19 on some of the engagement work, and then he  
20 supports Rob Schaul, who leads our analysis work  
21 in doing analysis activities, but he kind of  
22 cuts across all three.

23 **Q. And Rob Schaul is listed over there**  
24 **on the left side as analysis and response lead;**  
25 **correct?**

1 A. Yes.

2 Q. What does he do?

3 A. So he does a couple things, so one,  
4 he leads our engagement with international  
5 partners; two, he builds relationships with the  
6 research community, both in academia, across the  
7 federal government, as well as in the private  
8 sector; and then, three, he pulls that together  
9 to identify new reporting or research about MDM  
10 that might be of interest to the team; and then  
11 the fourth bucket of it is he helps develop kind  
12 of analytic type products.

13 So right now, for example, we're  
14 working on a risk framework to help our  
15 stakeholders understand how to determine if an  
16 MDM campaign is a risk to them or not.

17 So he would help kind of on that  
18 side of things.

19 Q. Okay. There was -- so he talks to  
20 international partners; who are they?

21 A. It varies. Generally, all of our  
22 engagements with international partners come  
23 through the State Department or the CISA  
24 international office.

25 We have engaged with NATO, G7 at

1 the kind of multilateral level, with the CFI,  
2 counter foreign interference forum, that  
3 includes several countries. And then we have  
4 different bilateral engagements. A lot of  
5 countries want to come and talk to us, and so  
6 we'll do basically MDM 101 for different  
7 countries at their request.

8 **Q. So this is both -- these are both**  
9 **foreign governments and foreign nongovernmental**  
10 **organizations?**

11 A. Yeah. I suppose if you consider  
12 the multilateral organizations, like NATO and G7  
13 as nongovernmental, but essentially we're only  
14 talking to government -- foreign government  
15 officials.

16 **Q. So the purpose of those discussions**  
17 **is to, what, track misinformation that is**  
18 **circulating in foreign countries that might come**  
19 **to the United States?**

20 A. No, that's not the purpose of the  
21 meetings.

22 **Q. Then what's the purpose?**

23 A. The purpose of the meetings is to  
24 share information about -- from a CISA  
25 perspective, share information about resilience

1 building. So there's some countries that are  
2 much more mature and have been doing it for a  
3 long time. So we try to learn from them kind of  
4 what they're doing, what works, what doesn't  
5 work.

6 So that's, again, from a CISA  
7 perspective, that's primarily our engagement  
8 with these groups.

9 **Q. And then you mentioned that**  
10 **Mr. Schaul coordinates with academic and**  
11 **research partners; is that correct?**

12 A. He doesn't coordinate, he builds  
13 relationships with, so that we can -- you know,  
14 if you have questions about reporting they put  
15 out or public reports that they have, public  
16 research, things like that, then we can have  
17 conversations with them about that research.

18 **Q. Who -- who -- who -- who do you**  
19 **have relationships like that with?**

20 A. We have relationships with a range  
21 of different entities. So from an academic  
22 standpoint, we've talked to folks at Harvard, at  
23 Clemson, University of Washington, Stanford, I  
24 believe we talked to people at Georgetown and  
25 American University, Michigan University,



1 University of Michigan.

2 Essentially, if there's an academic  
3 research that puts out a report that we think is  
4 of interest, and kind of reflects our work, we  
5 try to have conversations with them to try to  
6 understand what their research findings are, and  
7 in a non-profit stage, you know, the Alliance  
8 For Securing Democracy, the Digital Frameworks  
9 Research Lab -- sorry, for the court reporter, I  
10 know I'm talking quickly. So, you know, groups  
11 like that.

12 And then from a private sector  
13 perspective we talk to groups like Graphika,  
14 Alethia Group (phonetic), and organizations like  
15 those, who, again, kind of do that sort of work,  
16 mandates, you know, different organizations.

17 So again, the idea is to have a  
18 relationship with them so if they put out some  
19 reporting or some research publicly, that we can  
20 set up a meeting and kind of learn more about  
21 what they're seeing and what they're doing.

22 **Q. And has that kind of coordination**  
23 **gone on not from the last year but before the**  
24 **2020 election cycle?**

25 A. Yeah.

1 Q. And I think you mentioned a few  
2 entities there that includes Stanford and the  
3 University of Washington, Graphika; correct?

4 A. Correct.

5 Q. And all those organizations were --  
6 were involved in something called Election  
7 Integrity Partnership; right?

8 A. Yep.

9 Q. Yeah, what is the Election  
10 Integrity Partnership?

11 A. I mean, it's a collaboration  
12 amongst -- I believe in 2020 it's amongst those  
13 four -- amongst four organizations, to -- to  
14 better understand what was going on in the  
15 information environment around elections.

16 Q. And you say were those four -- you  
17 say those four organizations, I think I  
18 mentioned three, Stanford, University of  
19 Washington and Graphika, and was the Atlanta  
20 Council involved in that?

21 A. Yeah, I believe the Digital  
22 Forensic Research Lab was involved.

23 Q. And then were there other  
24 collaborators, besides those four, on the  
25 Election Integrity Partnership?

1           A.    I think those were the official  
2           members of the partnership.  I -- I don't know  
3           if you mean something different about  
4           collaborators.

5           **Q.    Well, let me ask this:  Was CISA --**  
6           **did CISA have any involvement in the Election**  
7           **Integrity Partnership?**

8           A.    Involvement in the sense that a  
9           couple of our interns came up with the idea and  
10          that we had some communications with them, yes.

11          **Q.    What kinds of communications did**  
12          **you have with them?**

13          A.    So we received some briefings on  
14          the work that they were doing.  And then, like I  
15          said, we had some interns that ended up working  
16          on it.  Those are principally -- principally the  
17          communications.

18                    We had some communications early on  
19          in the process, when they were making decisions,  
20          when Stanford was trying to figure out what the  
21          gap was.

22                    So yeah, so it was just general,  
23          like you would have with any other research  
24          organization.

25          **Q.    So it was no different than the**

1       **communications you had with other research**  
2       **organizations?**

3               A.    I think the one difference, I would  
4       say, is that we -- we probably connected them  
5       with other -- so we connected them with the  
6       Center For Internet Security, and we connected  
7       them with some of the election official groups,  
8       so the National Association of Secretaries of  
9       State and the National Association of State  
10      Election Directors, and then we facilitated some  
11      meetings between those three.

12              **Q.    Let me ask you this:  You said you**  
13      **had -- I take it you said some CISA interns came**  
14      **up with the idea; is that right?**

15              A.    Correct.

16              **Q.    And who are those interns?**

17              A.    I'm not going to give their names.

18              **Q.    Who were those interns?**

19              A.    Yeah, I'm not going to give those  
20      names.

21              **Q.    Who were -- you have no --**

22              A.    The Stanford students -- Stanford  
23      students have seen substantial amount of  
24      harassment from public reporting.  I'm not going  
25      to include my interns in that.

1 Q. Are you -- you're declining to  
2 answer the question without an instruction?

3 A. Correct.

4 Q. And you said those interns were  
5 also involved in the Election Integrity  
6 Partnership; correct?

7 A. I believe they worked for the  
8 Stanford Internet Observatory, as well, so yes.

9 Q. And they were working for CISA and  
10 Stanford Internet Observatory on the project?

11 A. When they came up with the idea,  
12 they -- obviously they were just interns. After  
13 their internships a couple of interns remained  
14 as interns. Several others went back to  
15 Stanford, as students, and did not remain as  
16 interns. Two of the interns ended up working on  
17 both in the fall; correct.

18 Q. You said two of the interns who  
19 were CISA interns, in the fall of 2020, worked  
20 on the Election Integrity Partnership; is that  
21 right?

22 A. They worked at the Stanford  
23 Internet Observatory, which was part of the  
24 Partnership.

25 Q. Were there any other interactions

1       **between CISA and the Election Integrity**  
2       **Partnership, that you're aware of?**

3               A.     So just to say so we had some  
4       initial conversation with the interns. We had a  
5       conversation with the Stanford Internet  
6       Observatory folks about the gap.

7               I believe we received a briefing  
8       from them, or two, on kind of what they were  
9       putting together.

10              We facilitated some meetings  
11       between Stanford folks, the Center For Internet  
12       Security, and election officials, where they had  
13       discussions about how they would work together.

14              And then I -- I'm sure we had some  
15       conversations, kind of throughout, when they  
16       were -- particularly when they were putting out  
17       public reporting about what they were seeing.

18              I wouldn't be surprised if there  
19       were some other kind of brief conversations in  
20       there, but I'm not recalling.

21              But those are generally the  
22       categories of the conversations we had.

23              **Q.     Did the Election Integrity**  
24       **Partnership, or a similar collaboration of any**  
25       **kind, operate during the 2022 election cycle?**

1 MR. GARDNER: Objection, vague.

2 BY MR. SAUER:

3 Q. You may answer.

4 A. So I believe the EIP did operate,  
5 but I'm not -- I'm not certain what they did.

6 Q. How do you know they operated in  
7 2022?

8 A. I believe they put out a public --  
9 some public reporting.

10 Q. Did you have --

11 A. But I --

12 Q. Go ahead.

13 A. We did not have communications with  
14 them. They gave us a briefing, early on, about  
15 what they were thinking about, and that was the  
16 extent of our communications with them on that  
17 stuff.

18 Q. When did that briefing occur?

19 A. I believe it was May/June of 2022.

20 Q. Who was at that briefing on your  
21 end, CISA?

22 A. On my end, it was me, I believe  
23 Geoff Hale. Who else was in that? I think one  
24 of our -- I think that may have been it, but  
25 there might have been one other staff person

1       there, as well. But it was primarily Geoff Hale  
2       and myself, that I recall.

3                   **Q. Who was in the briefing on the EIP**  
4       **side?**

5                   A. Renée DiResta was the lead, and  
6       then one of their staff, I believe his name was  
7       John, but honestly I forget what his name is.

8                   **Q. So just two people?**

9                   A. That I recall, yeah.

10                  **Q. What did they say in the briefing?**

11                  A. Essentially, they just walked  
12       through what their plans were for 2022, some of  
13       the lessons learned from 2020, that was  
14       essentially the gist of the conversation.

15                  **Q. What were their plans for 2022?**

16                  A. It sounded like they were going to  
17       do something similar to what they did in 2020 in  
18       terms of trying to support election officials.

19                  **Q. Did they indicate that they were**  
20       **coordinating with state and local election**  
21       **officials?**

22                  A. I think that was their goal with  
23       the -- with the work with state and local  
24       election officials. I'm not sure how they would  
25       describe it.



1 Q. Sorry, I think you said this  
2 earlier, and I can't remember.

3 When did this briefing occur, would  
4 you say it was in May or June of 2022?

5 A. I believe it was around that  
6 timeframe. My timeline recollections are awful,  
7 so I apologize for that, but I think it was  
8 around that timeline.

9 Q. Did you --

10 A. Things all blur together.

11 Q. Did they -- in fact, let me ask  
12 you: Did they invite CISA to participate again?

13 A. No. CISA didn't -- I mean, I  
14 wouldn't say CISA participated in 2020, so it  
15 wouldn't have been again, so it would have been  
16 participate for -- kind of for the first time.

17 Q. Did they invite CISA to have any  
18 role, at all, in what they were doing?

19 A. Not that I recall.

20 Q. Why were they giving you a  
21 briefing, then?

22 A. I think they should know our role  
23 in the federal government for election security.  
24 And we have, you know, an established  
25 relationship with them. So I think they were

1 just going around and making sure -- again, I  
2 don't -- I don't want to speak for them, but my  
3 sense was that they were just kind of briefing  
4 people who -- who were involved in election  
5 security at the federal level.

6 **Q. Do you -- do you know -- do you**  
7 **have any knowledge of what they actually did,**  
8 **after that briefing, during the 2022 election**  
9 **cycle?**

10 A. No. I know -- like I said, the  
11 reason I -- I think they were operating was  
12 there was a couple of public reports, one -- at  
13 least one public report, that I recall, that I  
14 thought was pretty good, but was it about  
15 specific disinformation, it was basically how to  
16 think about whether or not a narrative poses  
17 risks.

18 As I mentioned earlier, we were  
19 particularly interested in understanding how to  
20 determine if MDM creates risk. And we thought  
21 their products was pretty good on that.

22 **Q. You used a phrase earlier, that I**  
23 **did -- I passed over, and I didn't understand, a**  
24 **specific gap that we were talking about putting**  
25 **together the I&P in the first place. What's the**

1 **gap that you're referring to?**

2 A. Sure. So we had a conversation  
3 with the interns, and they were asking questions  
4 about kind of needs that the election officials  
5 have, generally.

6 One of the gaps that we identified  
7 from 2018 is, as you know, most election  
8 officials their offices are fairly low staff,  
9 low resourced, and so there was no -- they  
10 didn't have capabilities to try to identify  
11 disinformation targeting their jurisdictions,  
12 and so was essentially the gap is that most  
13 election offices throughout the country just  
14 didn't have that capacity or capability to be  
15 monitoring so that they could identify anything  
16 that would be potentially target their  
17 jurisdictions, so that was the gap.

18 **Q. So the gap is that state and local**  
19 **election officials don't -- just don't have the**  
20 **bandwidth or capacity to monitor mis and**  
21 **disinformation on social media that may affect**  
22 **their jurisdictions; right?**

23 A. Correct.

24 **Q. And then I take it was it the**  
25 **interns' idea that the Election Integrity**

1       **Partnership could be set up to kind of fill in**  
2       **that gap, was that the idea?**

3               A.    Again, I don't want to speak for  
4       the interns.  But at that point I don't think  
5       they were necessarily thinking about more of a  
6       partnership.

7               I think the conversation was more  
8       along the lines of this may be something that  
9       the Stanford Internet Observatory could look  
10      into, and then I think they went back and talked  
11      to their folks at the Stanford Internet  
12      Observatory and the idea was formed from there.

13              So I don't think that was the  
14      interns' initial thought was to have the EIP.

15              **Q.    Was there discussions of having**  
16      **CISA fill that gap, for example, by doing**  
17      **routing disinformation concerns to social media**  
18      **platforms?**

19              A.    With the -- there's no conversation  
20      with the interns about CISA filling the gap, no.

21              **Q.    How about internally to CISA, did**  
22      **CISA view itself as kind of helping fill that**  
23      **gap by, you know, helping state and local**  
24      **election officials addressing this mis and**  
25      **disinformation concern?**

1           A.    Our focus generally was not to play  
2           that role, no.  We -- we weren't looking to  
3           identify -- monitor social media to share with  
4           platforms.

5           **Q.    You mentioned that you -- I think**  
6           **you mentioned you put EIP in touch with CIS, the**  
7           **Center For Internet Security; is that right?**

8           A.    Correct.

9           **Q.    What is the Center For Internet**  
10          **Security.**

11          A.    I don't -- I don't know how to  
12          describe them.  They're essentially, as I  
13          understand it, they're non-profit that oversees  
14          the multi-state ISAC and the election  
15          infrastructure subsector information sharing and  
16          analysis center, that's what ISAC stands for, so  
17          that's my understanding of what they do.  I  
18          don't know what else they do.  I know them in  
19          those two contexts.

20          **Q.    And those two contexts are**  
21          **overseeing an ISAC, I-S-A-C, that involves**  
22          **multiple states; is that right?**

23          A.    Correct.

24          **Q.    Now, and that's a -- basically a**  
25          **sharing collaborative that they facilitate**

1       **amongst state and local election officials; is**  
2       **that right?**

3               A.     Yeah, it's a general woven artifact  
4     is information sharing with the sector. So each  
5     sector -- not each -- most sectors have their  
6     own information sharing and analysis center.  
7     They're independently stood up to serve those  
8     sectors.

9               And so CIS was the one who was  
10    responsible for kind of running the two that I  
11    mentioned.

12              **Q.     I'm sorry, what were those two, can**  
13    **you identify them again?**

14              A.     Sure. The multistate ISAC and the  
15    election infrastructure subsector ISAC. And  
16    just as a reminder of what ISAC is Information  
17    Sharing and Analysis Center.

18              **Q.     And those are, I think, referred to**  
19    **as the EI-ISAC and the MS-ISAC; is that right?**

20              A.     That's correct.

21              **Q.     And both of those, I take it,**  
22    **involve basically information sharing amongst**  
23    **state and local election officials; is that**  
24    **right?**

25              A.     I believe only the election

1 infrastructure one is focussed on -- on election  
2 officials. I believe the multistate one is  
3 broader across state and local government, but  
4 includes a broader set. I'm not sure if  
5 election officials are involved in the  
6 multistate.

7 **Q. Is the Center For Internet Security**  
8 **funded, in part, by CISA?**

9 A. To the best of my knowledge, CISA  
10 provides funding for the EI-ISAC.

11 **Q. Okay. And do you know how -- how**  
12 **is that funding provided, is it grants or how is**  
13 **it provided?**

14 A. I don't believe it's a grant, but  
15 I'm not 100 percent certain what the -- what the  
16 actual mechanism is, vehicle for the money to go  
17 there.

18 **Q. But they're --**

19 A. My understanding is that it's  
20 statutory, as well, but I could be wrong, also,  
21 so I don't want to speak too much.

22 **Q. But you're aware that CISA does**  
23 **provide funding for CIS to operate the EI-ISAC;**  
24 **is that right?**

25 A. My understanding is that they

1 provide funding to the EI-ISAC. I don't know if  
2 the goes -- if the EI-ISAC is an organization,  
3 and the money goes to them or if the money goes  
4 to CIS, and then they filter it down to the  
5 EI-ISAC. I'm not sure how it works, in  
6 practice.

7 **Q. Does CIS operate the EI-ISAC, I**  
8 **mean, does it kind of run it?**

9 A. Yeah, that's essentially how I see  
10 it, yeah.

11 **Q. And then you say you put them in**  
12 **touch, or CISA put the EIP in touch with CIS in**  
13 **2020, do you remember that?**

14 A. Yes.

15 **Q. How did that happen?**

16 A. So CISA's general position on -- on  
17 the switchboarding role was that it wasn't a  
18 role we necessarily wanted to play, because it's  
19 very resource intensive. And so we had been  
20 working with election officials to try to find  
21 an alternate way for them to have that role,  
22 somebody play that role.

23 They seemed to settle on the Center  
24 For Internet Security. And so since the EIP was  
25 working on the same mission, we wanted to make



1 sure that they were all connected.

2 Q. And so the same mission, I take it,  
3 is the switchboarding role that you've talked  
4 about before?

5 A. Correct.

6 Q. Yeah, so I take it CISA was playing  
7 a switchboarding role in 2020, but you mentioned  
8 that that's resource intensive and it wasn't  
9 something that you guys wanted to be principally  
10 responsible for; right?

11 A. Something we didn't want to be  
12 responsible for, at all. But election officials  
13 asked if we could continue serving in that role  
14 until they kind of got something else set up.

15 Q. And you did do that, right, in 2020  
16 you mentioned earlier that CISA performed a  
17 switchboarding function; right?

18 A. Correct, in 2020.

19 Q. And then Center For Internet  
20 Security performs a switchboarding function,  
21 too; is that right?

22 A. Yeah. So yes, yes and no. So yes  
23 in the sense they were receiving reporting  
24 directly from election officials. In the early  
25 part of 2020, they would forward what they were

1 receiving election officials to us at CISA, and  
2 then we would push that to the social media  
3 platform; as 2021 moved along, CIS more  
4 frequently provided that directly to the  
5 platforms, themselves.

6 And so I would say early on in the  
7 process, the switchboarding generally came  
8 through CISA. Later on in the process, it was  
9 more of a mixed bag of how the switchboarding  
10 worked.

11 **Q. And then did EIP play a**  
12 **switchboarding role, too?**

13 A. I believe EIP did report stuff to  
14 the platforms, themselves, yes.

15 **Q. And was there coordination between**  
16 **the switchboarders, so to speak, CISA and EIP**  
17 **and CIS?**

18 A. Most of the coordination was  
19 between CISA and the Centers For Internet  
20 Security.

21 There was a point where one of the  
22 platforms was concerned about too much kind of  
23 duplicate reporting coming in, and so we did  
24 have some conversations with EIP and CIS on how  
25 to kind of better manage that activity to make

1 sure we weren't overwhelming the platforms.

2 Q. In other words, like Twitter or  
3 Facebook would be hearing from CIS and CISA and  
4 EIP about a disinformation concern; correct?

5 A. Yeah. Generally speaking, yes,  
6 I'll just leave it there, yes, that's correct.

7 Q. And then --

8 A. Twitter, in particular, reached out  
9 to us and had some concerns about that.

10 Q. And I take you talked to EIP and  
11 talked to CIS about creating a more streamlined  
12 process through the platforms?

13 A. I don't think it was necessarily a  
14 streamlined process. We just wanted to make  
15 sure that there was -- that there was awareness  
16 for the platform.

17 So I think, to be honest with you,  
18 I don't recall how we ended up following this,  
19 in practice. But I think it was just we would  
20 let everybody know when we were setting  
21 something up through CIS. We would let CIS  
22 know, and I think CIS, through that  
23 relationship, would like EIP know.

24 But I don't recall, specifically,  
25 how we ended up kind of solving that problem.

1 Q. But at least there was, I guess,  
2 kind of communication among CISA, the EIP, and  
3 CIS about who was reporting various concerns in  
4 an attempt to kind of de-duplicate what's being  
5 sent to the social media platforms?

6 A. Yeah, I don't recall being directly  
7 from CISA to EIP. Like I said, I think we  
8 mostly worked it through CIS.

9 Q. Was there -- for example, was there  
10 direct e-mail communication between EIP and  
11 CISA?

12 A. I'm sure there was.

13 Q. I mean, was it your practice to  
14 copy the CISA's -- or sorry -- the EIP's tips,  
15 e-mail address when you were -- you or CIS was  
16 reporting a disinformation concern to a social  
17 media platform?

18 A. No, that was not standard practice.

19 Q. Did CIS do that?

20 A. I don't know. That's a good  
21 question. I don't know.

22 Q. Why don't we --

23 A. Just to be clear, you're -- sorry,  
24 just to be clear, you were asking if they were  
25 sending EIP when they sent e-mail to social

1 media platforms; correct.

2 Q. Yeah.

3 A. Yeah, I'm not sure. Sorry.

4 Q. When -- when was EIP copied by CIS  
5 or you on disinformation e-mails, if ever?

6 A. I don't believe we ever -- CISA  
7 ever copied EIS on e-mails we sent to platforms.  
8 I don't -- but where we were forwarding -- if we  
9 were forwarding something we received from an  
10 election official to the platform, I don't  
11 believe CISA ever copied EIP, certainly not to  
12 my recollection. It wasn't kind of our process.

13 I can't speak for the Center For  
14 Internet Security. I don't -- I don't recall  
15 who they were including on theirs.

16 Q. Did you notify EIP if you were  
17 flagging a disinformation concern for a social  
18 media platform in any way?

19 A. Not that I -- not directly, that I  
20 recall. We would -- we would generally copy the  
21 Center For Internet Security.

22 Q. Was it your understanding that they  
23 were communicating with EIP?

24 A. CIS? Yeah, that was essentially  
25 the -- their relationship was between those two,

1       yeah.

2                   **Q.     So in other words, you had the**  
3       **understanding that CIS had a relationship of**  
4       **communication and coordination with the Election**  
5       **Integrity Partnership; right?**

6                   A.     Yes.   Correct.

7                   **Q.     And then you would notify CIS if**  
8       **you were reporting something to a social media**  
9       **platform on the understanding that they were**  
10       **coordinating with EIP on what was being**  
11       **reported; correct?**

12                   A.     No.   The reason we -- we would  
13       coordinate with CIS was generally most of the  
14       reporting we received from an election official  
15       came through CIS.   And so we just wanted to let  
16       them know that we were -- we had set it up so  
17       that they had awareness of kind of where the  
18       report had gone.   And so that was the rationale  
19       for us coordinating with CIS.

20                   **Q.     And did you have the understanding**  
21       **that CIS was coordinating with EIP on what was**  
22       **being reported?**

23                   A.     I -- that would be speculating on  
24       exactly what they were doing there.   I'm not  
25       sure.

1 Q. You didn't know what they were  
2 doing?

3 A. I mean, I know they coordinated on  
4 things. I don't know the full nature of what  
5 they were coordinating on, I don't want to put  
6 words in their mouth.

7 (Exhibit No. 1 was marked for  
8 identification.)

9 MR. SAUER: Let's look at Exhibit  
10 1. I've sent that to your counsel.

11 MR. GARDNER: Yeah, we've got it up  
12 here.

13 BY MR. SAUER:

14 Q. Can you also see it on the screen  
15 share?

16 A. Yes.

17 Q. Are you familiar with this  
18 document?

19 A. Yes.

20 Q. In other words, is this the report  
21 that the Election Integrity Partnership did in  
22 2021, about its activities in the 2020 election?

23 A. Correct.

24 Q. Had you read it before or how did  
25 it get on your attention?

1 A. Yeah, I've read portions of it  
2 before, and some of the folks briefed us on it.

3 Q. Who are the folks that briefed you  
4 on it?

5 A. Alex Stamos and Renée DiResta.

6 Q. When did that briefing occur?

7 A. I'm sorry, when or where?

8 Q. When did that briefing occur?

9 A. It was late spring, early summer  
10 2021.

11 Q. This would have been around the  
12 time that the report was released?

13 A. Yeah, sometime after that.

14 Q. And Alex Stamos is at Stanford  
15 Internet Observatory; right?

16 A. Yes.

17 Q. Does he also serve on some CISA  
18 committees or subcommittees?

19 A. I don't know.

20 Q. Renée DiResta, is she also at  
21 Stanford -- Stanford Internet Observatory; is  
22 that right?

23 A. Yes. Yes, last I checked.

24 Q. Do you remember what they said in  
25 the briefing?



1 A. I think they just walked through  
2 kind of what they did and how they did it,  
3 explained what they kind of learned, how they  
4 viewed some of the issues, things like that.

5 Q. Who participated in the briefing,  
6 other than you, for CISA?

7 A. So I received a briefing when I was  
8 at the National Security Council. So it was a  
9 National Security Council colleague of mine,  
10 Marybeth Foley (phonetic).

11 Q. Did CISA receive a briefing?

12 A. I don't know for certain.

13 Q. Did you do -- I can't remember if  
14 you said this -- did you do a detail on the  
15 National Security Council in that timeframe?

16 A. From January 2021 to March 2022 I  
17 was on detail to the National Security Council.

18 Q. Why did they report to the National  
19 Security Council?

20 MR. GARDNER: Objection, calls for  
21 speculation.

22 BY MR. SAUER:

23 Q. You may answer.

24 A. Yeah, I don't know why.

25 Q. I mean, were they reporting back to

1       you because you had communicated with them back  
2       in 2020 or was it a report to your agency?

3                   MR. GARDNER: Objection, compound,  
4       calls for speculation.

5                   A.    Yeah, again, I don't -- I don't  
6       know why they -- why they wanted to brief us.

7                   Q.    Can you see the document on the  
8       screen share?

9                   A.    Yep.

10                  Q.    Scrolling down here on the third  
11       page of the document, they list the participants  
12       here. Are these the same participants that you  
13       talked about earlier?

14                  A.    Yeah.

15                  Q.    Yeah? And I think you mentioned  
16       Stanford Internet Observatory includes Alex  
17       Stamos and Renée DiResta; correct?

18                  A.    Yes.

19                  Q.    And then the University of  
20       Washington, Center For an Informed Public, is  
21       that where Dr. Kate Starbird works?

22                  A.    I believe so, yes.

23                  Q.    And is she also on a CISA  
24       subcommittee? Actually, isn't she on the MDM  
25       subcommittee for the CSAC?

1 A. I believe that's correct, yeah.

2 Q. And is she also involved in the  
3 Election Integrity Partnership?

4 A. Yeah, that's my understanding.

5 Q. Jumping ahead just a tiny bit, past  
6 the table of contents, here in the executive  
7 summary, on page six, little Roman six, you see  
8 here it says: Election Integrity Partnership  
9 was formed to enable realtime information  
10 exchange between election officials, government  
11 agencies, civil society organizations, social  
12 media platforms, the media, and the research  
13 community; correct?

14 A. Yeah, I see that sentence.

15 Q. There's a reference to both  
16 election officials and government agencies  
17 engaging in realtime information exchange with  
18 social media platforms; correct?

19 A. Yes.

20 Q. What -- do you know what government  
21 agencies engaged in realtime information  
22 exchange under the aegis of the EIP?

23 A. I don't know who they're referring  
24 to.

25 Q. Did CISA do that, at all? Did CISA

1       **share information with EIP?**

2           A.    Generally speaking, no.

3           **Q.    How about more specifically, did**  
4       **anyone at CISA share information with the EIP?**

5           A.    I mean, that's very broad. Did we  
6       share information? Can you be more specific  
7       about what type of information you're asking  
8       that we shared? We had conversations with them,  
9       so in that sense we shared information. Is  
10      there something in particular that you're asking  
11      about?

12          **Q.    Sure. What conversations did you**  
13      **have with them? I know you summarized them**  
14      **earlier, can you be more specific?**

15          A.    Yeah, I mean, I think that summary  
16      actually is -- is probably as specific as I can  
17      get. Like I said, we -- we had conversations  
18      with Stanford about the gap. They gave us some  
19      briefings on what they were doing, how they were  
20      doing it.

21                      Prior to the election, we had some  
22      conversations with them to facilitate and  
23      coordinate meetings, as I mentioned. And then  
24      when they put public reporting out, if we had  
25      questions about it, we would probably have

1 conversations with them around that, as well.

2 **Q. Was there any communication from**  
3 **government officials to EIP about specific**  
4 **disinformation concerns?**

5 A. Not that I'm aware of, no.

6 **Q. Who at CISA was involved in any**  
7 **interactions with the Election Integrity**  
8 **Partnership?**

9 A. In addition to the two interns, the  
10 primary interaction was myself and Matt  
11 Masterson.

12 **Q. Are you aware of anyone else at**  
13 **CISA communicating with them?**

14 A. It's possible, but I don't recall,  
15 and it certainly wouldn't have been -- you know,  
16 they would have just been part of a meeting with  
17 either Matt or myself.

18 **Q. How about Lauren Protentis, did she**  
19 **communicate?**

20 A. She wasn't part of the MDM team in  
21 2020.

22 **Q. How about --**

23 A. So she would not have been  
24 communicating them.

25 **Q. How about Geoff Hale?**

1           A.    I -- I wouldn't be surprised if  
2           Geoff was on some of the conversations, but I  
3           don't recall -- I don't recall him  
4           participating.

5           **Q.    How about Director Easterly? I**  
6           **guess she wasn't director back then. How about**  
7           **Director Krebs?**

8           A.    I believe Director Krebs had a  
9           relationship with Alex Stamos. So he may have  
10          had conversations in that context. I don't -- I  
11          don't believe he had -- necessarily had  
12          conversations in relation to EIP.

13          **Q.    And then, in fact, when he left**  
14          **CISA he joined Alex Stamos at the Stanford**  
15          **Internet Observatory or he joined Alex Stamos in**  
16          **some capacity, didn't he?**

17          A.    I believe they started a business  
18          together, yes.

19          **Q.    Do you know what that business was?**

20          A.    I'm sorry?

21          **Q.    Do you know what that business was?**

22          A.    I believe the name of it is  
23          Krebs -- Krebs/Stamos Group.

24          **Q.    Do you know what it does?**

25          A.    I believe cyber security theft.

1 I'm not entirely sure.

2 Q. Does it do anything related to  
3 misinformation and disinformation?

4 A. I don't know, if they do it hasn't  
5 been something they've been promoting, that I'm  
6 aware of.

7 Q. Are you aware of any communications  
8 between Director Krebs -- Krebs and Alex Stamos  
9 while he -- while Krebs was still director?

10 MR. GARDNER: Objection, vague.

11 A. Yeah, it's really vague.

12 Again what --

13 Q. Any communications is broad and not  
14 vague.

15 I want to know if you have any  
16 communications of any kind between Director  
17 Krebs and Alex Stamos when Krebs was still  
18 director of CISA?

19 MR. GARDNER: Same objection.

20 A. I believe they -- Director Krebs  
21 may have participated in a couple of meetings  
22 that I'm aware of, that Stamos was also in, but  
23 beyond that I'm -- I'm not familiar with --  
24 obviously not going to be familiar with Krebs's  
25 direct communications with Stamos.

1                   **Q.    What meetings were they both**  
2                   **involved in, if you recall?**

3                   A.    So I can recall an event that  
4                   occurred out in Stanford, that Krebs spoke at  
5                   for the Stanford Internet Observatory, for  
6                   example. I believe the first government  
7                   industry sync Stamos was the Facebook lead, at  
8                   the time. This was before he went to Stanford  
9                   Internet Observatory, and Director Krebs  
10                  participated in that meeting, so meetings like  
11                  that.

12                                Beyond that, I don't have a real  
13                   understanding of how they communicated with each  
14                   other.

15                   **Q.    Was there any discussion of the**  
16                   **Election Integrity Partnership at the meetings**  
17                   **you're aware of?**

18                   A.    Not that I'm aware of, no.

19                   **Q.    Turning back to the screen share,**  
20                   **it talks about election officials, engaging in**  
21                   **realtime information sharing with social media**  
22                   **platforms, among others; do you see that?**

23                   A.    Yeah, as part of that same  
24                   sentence, right; is that what you're referring  
25                   to?



1 Q. Yeah.

2 A. Yeah.

3 Q. Are you aware of state and local  
4 election officials engaging in realtime  
5 information sharing with the election  
6 integrity -- you know, with social media  
7 platforms through the Election Integrity  
8 Partnership?

9 A. I -- I don't know the relationship  
10 between EIP and election officials. I'm not  
11 sure if they're referring to direct reporting to  
12 them from election officials or if they're  
13 referring to reporting through the Center for  
14 Internet Security, I'm just not sure what  
15 they're referring to there.

16 Q. How about through the Center For  
17 Internet Security, was there election reporting  
18 through them?

19 A. Yeah, so generally speaking, the  
20 reporting that CISA received came through the  
21 Center For Internet Security.

22 Q. Gotcha.

23 And how about -- did -- did --  
24 as -- to the extent you understand, did EIP  
25 receive reporting through the Center of Internet

1       **Security, you know, kind of from election**  
2       **officials through the internet security to the**  
3       **Election Integrity Partnership?**

4                   MR. GARDNER: Objection, lack of  
5       foundation.

6       BY MR. SAUER:

7                   **Q. You may answer. Do you know if --**

8                   A. Yeah, I -- I'm not -- I'm not sure  
9       what their full relationship was and how they  
10      were sharing, what the specifics were. It  
11      wouldn't surprise me if CIS had shared some with  
12      EIP, but I just don't know.

13                  **Q. You mentioned Matt Masterson, and I**  
14      **think you said that he was involved in briefing**  
15      **with the EIP; is that correct?**

16                  A. No. He was involved -- involved  
17      in -- in conversations with Stanford Internet  
18      Observatory. He probably -- generally, all of  
19      our -- so just to take a step back, generally  
20      our communications, when VIPs stood up, were  
21      still at the Stanford Internet Observatory.

22                  So the conversations I'm aware of  
23      with Masterson were generally at the Stanford  
24      Internet Observatory. He was also briefed -- I  
25      seem to recall he was probably in some of the

1 briefings I was in or conversations when we had  
2 questions about reporting that they did, public  
3 reporting.

4 So I don't know how to kind of  
5 thread the needle between, you know, when they  
6 were just conversations with Stanford Internet  
7 Observatory and when they would be considered  
8 conversations with the EIP.

9 Q. And that, I take it, you said  
10 thread the needle, I take it that's kind of a  
11 fuzzy distinction, because the EIP is a  
12 collaboration that involves the Stanford  
13 Internet Observatory; correct?

14 A. Right.

15 Q. Do you know -- do you know -- let  
16 me ask you this: What discussions do you know  
17 of between Matt Masterson and Stanford Internet  
18 Observatory that related in any way to the EIP?

19 A. I think it would have just been if  
20 we had questions about public reporting.

21 Q. What is --

22 A. Kind of once they were up and  
23 running.

24 So he was involved in some of the  
25 conversations before, you know, the first couple

1 that I talked to about, kind of in our  
2 engagement with Stanford Internet Observatory,  
3 he was involved, I know, in at least one of the  
4 conversations about that.

5 And then, after that, I don't think  
6 he was particularly involved, but he may have  
7 been involved, and we had some briefings for --  
8 or not briefings, I don't think is the right  
9 word, where we had conversations with them about  
10 public reporting we put out.

11 **Q. When you say public reporting, what**  
12 **do you mean?**

13 A. So the EIP put out regular kind of  
14 blog posts, excuse me, regular blog posts on  
15 what they were seeing, so -- so it was publicly  
16 available information.

17 **Q. And -- and did you -- did they**  
18 **discuss, you know, those blog posts with Matt**  
19 **Masterson or you before they were posted?**

20 A. Not that I recall.

21 **Q. And what discussions did you have**  
22 **with the public reporting?**

23 MR. SCOTT: John, just one second,  
24 it looks like the video is frozen on our end.  
25 Does it appear frozen on your end, as well.

1 MR. SAUER: I see a little  
2 interference. Shall we go off the record?

3 THE WITNESS: There's interference  
4 with the top and the bottom. I'm not seeing  
5 that. Still, we can go off -- we can go off the  
6 record and try to fix that.

7 MR. SAUER: Let's go off the  
8 record.

9 THE VIDEOGRAPHER: The time is now  
10 10:27. We are off the record.

11 (Recess.)

12 THE VIDEOGRAPHER: The time is now  
13 10:40. We are back on the record.

14 BY MR. SAUER:

15 Q. Mr. Scully, I think we were talking  
16 about Matt Masterson before we had the  
17 technical -- technical difficulty.

18 Generally speaking, do you know  
19 what role he had, if any, in originating the  
20 concept for the Election Integrity Partnership?

21 A. So his primary role was the same as  
22 mine, in terms of just clarifying the gap that  
23 election officials faced for the folks at the  
24 Stanford Internet Observatory early on in the  
25 process.

1 Q. And is that something that you  
2 discussed with the interns when they came up  
3 with the idea? Did the interns come to you or  
4 Mr. Masterson and talk about the gap?

5 A. I'm sorry, so are you referring  
6 specifically to the gap?

7 Q. Yeah.

8 A. Yeah, so the gap came from our --  
9 the gap came from myself.

10 Q. That was your idea, that there is a  
11 gap, and you shared that with the interns?

12 A. I'm not sure I would say that was  
13 my idea. That was -- that was just kind of from  
14 lessons learned from 2018, I think across the  
15 election community.

16 I don't know that I would say that  
17 that was -- that was something that we came up  
18 with on our own.

19 Q. Is that something you shared with  
20 the interns?

21 A. It is something I shared with the  
22 interns, correct.

23 Q. And then the interns came up with  
24 the idea of putting together the Election  
25 Integrity Partnership as a way of assisting

1       **state and local election authorities of filling**  
2       **that gap; right?**

3               A.     I don't -- I don't know what the  
4       exact process was, essentially they identified  
5       the gap. They went back and talked to the folks  
6       at the Stanford Internet Observatory. And  
7       somewhere in that sausage making process, along  
8       the way, they decided that this partnership  
9       would be the best approach to take.

10              **Q.     In that timeframe, did they also**  
11       **have discussions with you about putting together**  
12       **something like this?**

13              A.     I'm sure they mentioned it to us  
14       somewhere along the line, that this was  
15       something they were thinking about, but I  
16       don't -- I don't know that it went beyond that.

17              **Q.     How about Mr. Masterson, did they**  
18       **discuss it with him?**

19              A.     Again, I'm not familiar with all of  
20       Matt's communications with these folks, but he  
21       was in the meeting where we talked about the gap  
22       with Stamos, in particular. And I believe  
23       Stamos mentioned that as an option during that  
24       call. I don't know if he had any other  
25       conversations with them. I don't know about

1 that.

2 Q. When did that meeting with Alex  
3 Stamos occur?

4 A. Sometime in the summer of 2020, it  
5 would have -- yeah, I don't know. The exact  
6 date would be hard for me to figure out, sorry.  
7 Yeah, the interns -- sorry -- the interns  
8 probably arrived in the May timeframe, so we  
9 probably would have had had that conversation --  
10 the initial conversation sometime in June. And  
11 then probably Stamos, you know, a week or two  
12 after that, so probably June/July, I would say.

13 Q. Was Mr. Masterson in the meeting  
14 where you discussed the gap with the interns?

15 A. Not that I recall, no.

16 Q. What did Mr. Stamos say in this  
17 meeting you recall from the June to July  
18 timeframe of 2020?

19 A. Essentially, he just wanted to  
20 confirm that we agreed with the interns that  
21 this was a gap.

22 Q. What -- what was said about the gap  
23 in that meeting, that you remember?

24 A. Yeah, it was basically along the  
25 lines he just said, hey, the interns told me



1 that there's a gap for election officials where  
2 most of them don't have the resources to do --  
3 to identify disinformation that may be targeting  
4 their jurisdictions, is that -- did the interns  
5 give me that information correctly. He was  
6 thinking about potentially doing something, and  
7 he obviously didn't want to spend time and  
8 resources doing something if there wasn't, in  
9 fact, a gap.

10 **Q. How long did this meeting occur or**  
11 **last, do you think?**

12 A. That's all of maybe 10 or 15  
13 minutes.

14 **Q. Was there any other communications**  
15 **with Mr. Stamos during this timeframe?**

16 MR. GARDNER: Objection, vague,  
17 also calls for speculation.

18 BY MR. SAUER:

19 **Q. Do you remember any?**

20 A. So I don't recall any conversations  
21 I had with him in that timeframe. I obviously  
22 can't speak for Masterson.

23 **Q. Okay. Scroll ahead to page XII.**  
24 **There's a thank you there for contributors, and**  
25 **you see Kate Starbird is on that list; do you**

1 see that? You can look at the screen share.

2 A. Yes.

3 Q. You're there? Yeah, do you know --

4 A. Yeah, I got it.

5 Q. Do you know how she contributed to  
6 the Election Integrity Partnership?

7 A. I don't.

8 Q. And I see Alex Stamos up here,  
9 obviously kind of set the thing off; right? Do  
10 you know how else he was involved?

11 A. I don't.

12 Q. Okay. Down here it says the  
13 Election Integrity Partnership would like to  
14 thank Matt Masterson for additional feedback; do  
15 you see that?

16 A. I do.

17 Q. Do you know what feedback  
18 Mr. Masterson provided to the Election Integrity  
19 Partnership?

20 A. I don't.

21 Q. When did Mr. Masterson leave CISA  
22 and go to Microsoft?

23 A. So Matt left CISA, I believe, in  
24 January 2021. I don't think he started at  
25 Microsoft until early 2022.

1 Q. Oh, do you know what he did in the  
2 intervening year?

3 A. I believe he -- he worked -- he was  
4 a fellow at the Stanford Internet Observatory.

5 Q. Oh, so he went from CISA to work  
6 with Alex Stamos's group at the Stanford  
7 Internet Observatory?

8 A. That's my understanding, yes.

9 Q. And Mr. Masterson is thanked here,  
10 in this spring of 2021, I take it he was at the  
11 Stanford Internet Observatory by then?

12 A. I don't know when he officially  
13 started.

14 Q. I'm going to jump ahead to page 2  
15 of the executive summary. So if you're  
16 following on the PDF it would be the 20th page  
17 of the PDF.

18 There's a discussion here where it  
19 says: The initial idea for the partnership came  
20 from four students that the Stanford Internet  
21 Observatory funded to complete volunteer  
22 internships at CISA; right?

23 A. Correct.

24 Q. Okay. You've declined to identify  
25 them, early in your testimony. Do you know who

1       they are? Who are those four students? Do you  
2       know who they are?

3               A. I know for certain who two are, I  
4       believe I know who the third is, I'm unsure who  
5       the fourth is.

6               Q. What -- what were they doing in  
7       their internships for CISA at the time they  
8       originated this idea?

9               A. They had different activities, so  
10      they supported across the election security  
11      initiative, broadly. So trying to think if I can  
12      recall specific tasks that they had.

13              Q. And then, if you look to the next  
14      two sentences, it talks about responsibilities  
15      for election information security is divided  
16      across government offices, and it goes on to say  
17      that, yet, no government agency in the United  
18      States has the explicit mandate to monitor and  
19      correct election mis and disinformation;  
20      correct?

21              A. I'm sorry, is that the next page?

22              Q. If you look at the screen share,  
23      can you read that? I can zoom in, if that  
24      helps.

25                      MR. GARDNER: A few sentences below

1 where he was reading.

2 THE WITNESS: Okay. Got you.

3 BY MR. SAUER:

4 Q. So it says: Yet, no government  
5 agency in the United States has the explicit  
6 mandate to monitor and correct misinformation  
7 and disinformation; correct?

8 A. Sorry, I'm just trying to read and  
9 catch up.

10 Q. I'm just asking if you see where it  
11 says that.

12 A. Yeah, I see where it says that.

13 Q. And it seems to me that they're  
14 talking about a slightly different gap than the  
15 one you talked about earlier; right? They're  
16 saying there's a gap in federal government  
17 authority to monitor and correct election mis  
18 and disinformation, right, as opposed to a gap  
19 among the capacity for state and local election  
20 authorities to do it; right?

21 A. To be honest, I don't know what  
22 they're referencing, so I don't -- I don't want  
23 to speculate on what they're trying to say  
24 there.

25 Q. Let me ask you this: Do you think

1       **there's a gap in the authority of federal**  
2       **government agencies to monitor and correct**  
3       **election mis and disinformation?**

4                   MR. GARDNER: Objection to the  
5       extent it calls for a legal conclusion.

6 BY MR. SAUER:

7                   **Q. Do you think that?**

8                   A. Yeah, I'm not a -- I'm not a  
9       lawyer, I don't want to comment on the legal  
10      authorities of the departmental agencies.

11                  **Q. I'm just asking whether you**  
12      **think -- I'm not asking for your legal**  
13      **conclusion, I'm asking whether you think there's**  
14      **a gap in the authority of federal agencies that**  
15      **makes them unable to monitor and correct mis and**  
16      **disinformation?**

17                  MR. GARDNER: Same objection, calls  
18      for a legal conclusion.

19                  A. Yeah, by definition, an authority  
20      is a legal determination I'm not comfortable  
21      making.

22                  **Q. Let me ask you this: As a**  
23      **practical matter, do you believe there's a gap**  
24      **in the ability, as opposed to the authority, the**  
25      **ability of federal government agencies to**

1           **monitor and correct mis and disinformation?**

2                           MR. GARDNER: Objection, vague.

3 BY MR. SAUER:

4                   **Q. You may answer.**

5                   A. Yeah, can you clarify exactly what  
6 you're asking? I just want to make sure I  
7 understand what you're trying to get at.

8                   **Q. I'm using your word, a gap; right?**

9                   A. Yes.

10                   **Q. You just called it a gap, earlier,**  
11 **and that's a practical word, it's not a legal**  
12 **conclusion?**

13                   A. Correct.

14                   **Q. So I'm asking you, you talked about**  
15 **a gap with respect to the capacities of state**  
16 **and local election authorities; correct?**

17                   A. That's correct, yeah.

18                   **Q. Do you think there's a similar gap**  
19 **with respect to the ability of federal**  
20 **government agencies to respond to mis and**  
21 **disinformation on social media?**

22                   MR. GARDNER: Same objection,  
23 vague.

24                   A. I -- I think the federal government  
25 certainly would have the capability, if it chose

1 to use it, and had the authority to do it.

2 Q. Do you think it hasn't chosen to  
3 use that capability?

4 A. So generally speaking, I'm trying  
5 to understand your question. So is there a gap  
6 in the federal government's ability to, what, to  
7 provide information on social media about what's  
8 online on their platforms, is that what you're  
9 asking?

10 Q. I'm asking if there was a gap in  
11 the federal government's ability to, you know,  
12 take any kind of action to correct mis and  
13 disinformation on social media?

14 MR. GARDNER: Same objection, to  
15 the extent it calls for a legal conclusion.

16 A. Yeah, I don't know that there's a  
17 gap in the federal government's ability to do  
18 it.

19 Q. Well, let me ask this: It goes on  
20 to say -- let me ask you this: This notion that  
21 the report says that no government agency in the  
22 United States has the explicit mandate to  
23 monitor and correct election mis and  
24 disinformation, is that something that was  
25 discussed with the CISA interns who originated



1 the EIP?

2 A. Not that I recall, no.

3 Q. Do you remember any discussions of  
4 that with anyone else, suggesting that, you  
5 know, there's no government agency in United  
6 States with an explicit mandate to monitor and  
7 correct election mis and disinformation?

8 A. No, not that I -- not that I  
9 recall. It's possible, though.

10 Q. It goes on to say: This is  
11 especially true for election disinformation that  
12 originates from within the United States, which  
13 would likely be excluded from law enforcement  
14 action under the first amendment, is not  
15 appropriate for study by intelligence agencies  
16 restricted from operating in the United States;  
17 connect?

18 A. That's what the sentence says, yes.

19 Q. Do you agree with that sentence?

20 MR. GARDNER: Objection, calls for  
21 a legal conclusion.

22 BY MR. SAUER:

23 Q. Do you?

24 MR. GARDNER: Same objection.

25 A. I'm sorry, I'm reading the

1 sentence.

2 Yeah, this definitely gets into  
3 legal authority stuff that I would not want to  
4 comment on.

5 Q. And the next sentence says: As a  
6 result, during the 2020 election local and state  
7 election officials, who had a strong partner on  
8 election system and overall cyber security  
9 efforts in CISA, were without a clearinghouse  
10 for assessing mis and disinformation targeting  
11 their voting operations; correct?

12 A. Yeah, that's what this sentence  
13 says.

14 Q. That, to me, sounds like it's  
15 talking about the same gap you talked about  
16 earlier, and that's state and local election  
17 officials were without a clearinghouse for  
18 assessing mis and disinformation targeting their  
19 voting operations; right?

20 A. That's how I read that sentence,  
21 yeah.

22 Q. Yeah, and I take it that this  
23 report links that gap to gaps that they perceive  
24 in federal authority; right?

25 MR. GARDNER: Objection, calls for

1 speculation.

2 A. Yeah, I don't want to speculate on  
3 what they're trying to do there.

4 Q. Okay. Next sentence says:  
5 Students approach SIO leadership in the early  
6 summer, and in consultation with CISA and other  
7 stakeholders a coalition was assembled with  
8 like-minded partner institutions; do you see  
9 that?

10 A. I do.

11 Q. What -- let me ask you this: It  
12 says, in consultation with CISA, what  
13 consultation with CISA do you recall relating to  
14 the assembling of this coalition?

15 A. I don't recall any consultation  
16 with relation to the assembly of the coalition.

17 Q. Well, you don't recall anyone  
18 consulting with CISA about putting together the  
19 Election Integrity Partnership?

20 MR. GARDNER: Objection,  
21 mischaracterizes the witness's previous  
22 testimony.

23 A. Yeah, so I don't recall any  
24 consultation with us about who would be involved  
25 in the -- in the EIP, who their members would be

1 or anything like that.

2 Q. Do you remember any consultation of  
3 any kind about starting up the EIP in any  
4 connection?

5 A. Just what I referred to earlier,  
6 the conversations with the interns and the  
7 conversation with Stamos about verifying the gap  
8 existed.

9 Q. How about Mr. Masterson, is it  
10 possible they consulted with him?

11 MR. GARDNER: Objection, calls for  
12 speculation.

13 A. Yeah, I don't know what  
14 conversations Matt had with them.

15 Q. Do you know whether he had any  
16 conversations with them relating to the  
17 commencement of the EIP?

18 A. I don't.

19 Q. And the next page of the document,  
20 they provide an operational timeline; do you see  
21 that?

22 A. I do.

23 Q. And here, the second entry in their  
24 operational timeline, is -- I'm having trouble  
25 highlighting -- it says: July 9th of 2020,

1 meeting with CISA to present EIP concept; do you  
2 see that?

3 A. Yep, I see that.

4 Q. Do you know what meeting that is  
5 referring to?

6 A. I don't know specifically what  
7 meeting that's referring to, no.

8 Q. Would that -- to your mind, would  
9 that describe the 10 to 15 minute phone call you  
10 had with Alex Stamos about the gap that you  
11 talked about earlier? Would you have described  
12 that phone call as a meeting with the EIP for  
13 EIP to present -- for -- to present the EIP  
14 concept to CISA?

15 A. That 10 to 15 minute phone call  
16 only included Stamos, that I recall. So I don't  
17 know that I would frame it as a meeting to  
18 present the EIP concept.

19 As I mentioned earlier, he did kind  
20 of raise the possibility of setting up some sort  
21 of a partnership, during that call, so that  
22 could be what his -- what his thinking was, but  
23 I don't know what he's referring to there.

24 Q. What kind of a partnership did he  
25 talk about in that call?

1           A.    He just said he thought he -- he  
2           was thinking about potentially just getting  
3           other -- other similar institutions involved.

4                    I don't recall it -- I don't even  
5           recall if he mentioned any names or not. I  
6           think it was more of a generic, where he didn't  
7           think Stanford could necessarily do it on its  
8           own, and would consider kind of forming some  
9           sort of partnership.

10           **Q.    Did he talk about forming any kind**  
11           **of partnership with CISA?**

12           A.    No.

13           **Q.    So he didn't ask CISA to play any**  
14           **role in the concept he was putting together?**

15           A.    No. Again, beyond -- sorry, just  
16           to -- beyond what I've talked about earlier, you  
17           know, I think he knew he would need us helping  
18           him connect with election officials.

19           **Q.    So he -- to the extent he -- okay.**  
20                    **So he was asking for your help in**  
21           **connecting with election officials in that**  
22           **meeting?**

23           A.    I believe that was one of the asks,  
24           but I don't -- it could have been then, it could  
25           have been at another time, if that happened.

1 Q. Is there a later conversation with  
2 Mr. Stamos?

3 A. I don't recall, but that's what I  
4 think there was a fifth call. But again, I  
5 don't -- you know, this was several years ago,  
6 and my memory's a little foggy on timelines and  
7 everything that happened.

8 Q. But to the best of your  
9 recollection, at some point he asked for CISA's  
10 assistance in connecting with state and local  
11 election officials; right?

12 A. Yeah.

13 Q. Is that when you put him in touch  
14 with the Center For Internet Security?

15 A. I think they way initially put him  
16 in touch with the National Association, so the  
17 two I mentioned earlier, the National  
18 Association of Secretary's of State, and the  
19 National Association of State Election  
20 Directors. I'm not entirely -- I don't recall  
21 when, exactly, Center For Internet Security got  
22 involved.

23 Q. At some point, did you put him --  
24 put him in touch with CIS?

25 A. So we put the Stanford Internet

1 Observatory in touch with them. I forget if it  
2 was Alex, himself, or if it was somebody from  
3 the team there.

4 Q. So at some point you put them in  
5 touch with CIS. And were you involved in  
6 further communications with CIS and anyone at  
7 EIP?

8 A. Yeah, so as I mentioned earlier, I  
9 facilitated some meetings between them, involved  
10 between them and election officials.

11 Q. What sort of -- can you unpack that  
12 a little bit, you facilitated some meetings  
13 between -- was that both EIP and CIS?

14 A. Right. So I facilitated meetings,  
15 some meetings between EIP and CIS to make sure  
16 that they were -- they didn't have relationship  
17 before the -- they didn't know each other.

18 So we just facilitated getting them  
19 together to talk and figure out how they were  
20 going to work together.

21 Q. Got you. And who was at those  
22 meetings from EIP?

23 A. I don't recall.

24 Q. How about CIS, who did you put them  
25 in touch with at CIS?



1           A.    I only recall the CIS person's  
2           first name was Aaron. I'm blanking on his last  
3           name, at this point. I suspect there were other  
4           people from CIS on the call, as well, but he  
5           was -- Aaron was my principal contact at CIS.  
6           And that's Aaron, A-a-r-o-n.

7           **Q.    And I take it the purpose of that**  
8           **meeting was to set up a direct line of**  
9           **communication between CIS and EIP?**

10          A.    Correct.

11          **Q.    And then did you mention that you**  
12          **facilitated other meetings, for example, between**  
13          **EIP and NASED or National Association of**  
14          **Secretaries of State?**

15          A.    Yeah, my recollection is that we  
16          did facilitate. We put them in contact. I  
17          don't -- I don't know if we were on the calls or  
18          not, I don't recall, but -- but I seem to recall  
19          we did put them in contact.

20          **Q.    Okay. And specifically you mean**  
21          **you put EIP --**

22          A.    EIP in.

23          **Q.    -- in contact with NASED and NASOS;**  
24          **is that what it's called?**

25          A.    Just NASS, but yes.

1 Q. Okay. And so, yeah, sorry, for  
2 clarity, you put EIP in contact with both NASED  
3 and NASS; correct?

4 A. And just to be clear, we put SIO  
5 folks in contact with them.

6 Q. Okay.

7 A. But they were part of EIP, so  
8 that's kind of the -- I don't know when EIP was  
9 stood up in relation to the conversations,  
10 because I don't really know when the  
11 conversations occurred, either. So just so  
12 you're clear, we worked through the SIO when we  
13 made those connections.

14 Q. Got you. Do you remember who at  
15 the SIO was involved in those connections?

16 A. I don't.

17 Q. And again, SIO is short for  
18 Stanford Internet Observatory; correct?

19 A. Correct.

20 Q. Do you know, what was the timeframe  
21 of those, you know, connections that you  
22 facilitated with, you know, Stanford Internet  
23 Observatory folks and CIS, NASED and NASS?

24 A. I don't know for certain, but I  
25 would guess they were late July or August.

1 Q. So this would have been around the  
2 time that the EIP is kind of ramping up its  
3 activities?

4 A. Yeah, I don't -- I mean, I don't  
5 know when they were ramping up their activities,  
6 but I would assume it was around that time.

7 Q. Let me scroll down, so you can see  
8 this on the screen share, it's page 8. Is that  
9 size on the screen share visible to you?

10 A. Somewhat.

11 Q. Do you see here on page 8 there's a  
12 kind of graphic where the EIP report lists four  
13 major stakeholders, government, civil society,  
14 platforms and media; right?

15 A. Yep, I see that.

16 Q. You got an arrow from government, a  
17 black arrow that flows from government to intake  
18 queue; correct?

19 A. Yep.

20 Q. Do you know what that's referring  
21 to, did the government -- do you know what  
22 governments as stakeholders submitting  
23 information for the intake queue for the EIP?

24 A. I don't know if, specifically, what  
25 that's in reference to, no. I mean, I would

1 think it was election officials, but I don't --  
2 I don't know.

3 **Q. How about CISA, would CISA ever**  
4 **receive a report from election officials and**  
5 **pass it along to EIP?**

6 A. I don't recall us doing that. It  
7 wasn't part of our process, and -- and we would  
8 just send it to the platforms, ourselves, so I  
9 don't know that we would send it to EIP.

10 **Q. How about CIS, do you know if they**  
11 **did that on behalf of state and local officials?**

12 A. Did CIS forward messages that  
13 election officials sent to them to EIP?

14 **Q. Yeah, about disinformation.**

15 A. I would think so, but I don't know  
16 for certain.

17 **Q. And you see there's a red arrow**  
18 **down here at the bottom, from tier 3:**  
19 **Mitigation, and then that flows back to**  
20 **government.**

21 **Were you aware of EIP reporting**  
22 **back to CISA about what happened with**  
23 **disinformation or misinformation reports?**

24 A. I don't recall that there was  
25 communication when -- so just let me take a step

1 back. So you're asking if we were familiar with  
2 when EIP would send reports to the platforms,  
3 were we aware of that?

4 **Q. Correct.**

5 A. Generally speaking, we were not --  
6 as far as I know we were not aware. I wouldn't  
7 say generally.

8 As far as I'm aware, we were not in  
9 the loop when they were communicating with  
10 platforms.

11 **Q. And I apologize, I split the screen**  
12 **on screen share. Actually, stay with that**  
13 **graphic for a minute. Up here in the corner, it**  
14 **says, tier one: Detection intake. On-call data**  
15 **gathering, triage, and response; do you see**  
16 **that?**

17 A. I do.

18 **Q. Do you know how the Election**  
19 **Integrity Partnership gathered data about what**  
20 **was being said on social media in 2020?**

21 A. I don't know the specifics of how  
22 they did that, no.

23 **Q. Did you have any understanding at**  
24 **all, other than obviously receiving reports from**  
25 **CIS, NASED and NASS?**

1 A. My understanding was that they  
2 monitored social media in some way.

3 Q. Yeah, do you have any idea how they  
4 did it? I mean, there's different ways of doing  
5 that, do you know how they did it?

6 A. I don't know what tools or  
7 capabilities they used, no.

8 Q. Down here below the graphic, it  
9 talks about tickets being submitted to the EIP,  
10 it says tickets were submitted both by trusted  
11 expert stakeholders detailed in section 1.4 on  
12 page 11, an internal EIP analysts; correct?

13 A. Yes.

14 Q. Do you know who the trusted  
15 external stakeholders were?

16 A. I don't.

17 Q. Do you know whether CISA, at least  
18 EIP considered CISA a trusted external  
19 stakeholder?

20 MR. GARDNER: Objection, calls for  
21 separation.

22 BY MR. SAUER:

23 Q. Do you know.

24 A. I suspect if we scroll down to page  
25 11 we'll find out who the stakeholders were.

1 Q. Good idea. So here at the bottom  
2 of page 11, section 1.4, discussing external  
3 stakeholders; do you see where we are?

4 A. Getting there. And 11, external  
5 stakeholders. Yep.

6 Q. It says: The EIP serve as a  
7 connector for many stakeholders, who both  
8 provided inputs and received outputs; correct?

9 A. Yep.

10 Q. Okay. And then flipping to the  
11 next page, 12, first sentence: External  
12 stakeholders include government, civil society,  
13 social media companies, and news media entities;  
14 correct?

15 A. Correct.

16 Q. It says: Government and civil  
17 society partners could create tickets or send  
18 notes to EIP analysts; right?

19 A. That's what it says, yes.

20 Q. It goes on to say: They use these  
21 procedures to flag incidents to be emerging  
22 narratives to be assessed by EIP analysts;  
23 correct?

24 A. That's what it says, correct.

25 Q. And do you know what government's

1 partners were creating tickets to flag incidents  
2 or merging narratives to the EIP?

3 A. I don't.

4 Q. Immediately below that paragraph,  
5 they mention some government officials; right?

6 A. Yep.

7 Q. Right there, it says: Four major  
8 stakeholder groups in that graphic in the middle  
9 of page 12; right?

10 A. Yep.

11 Q. And there's three that are listed  
12 there; right?

13 A. Mm-hmm.

14 Q. There's Election Infrastructure  
15 ISAC; right?

16 A. Correct.

17 Q. And that's the EI-ISAC that CISA  
18 funds the Center For Internet Security to  
19 operate; is that right?

20 A. Again, I don't know if the money  
21 goes directly to the EI-ISAC. I don't know how  
22 the money flows, but EI-ISAC is part of CIS and  
23 we do fund the EI-ISAC.

24 Q. Yeah, and then the next one listed  
25 is CISA?



1 A. Mm-mmm.

2 Q. And the next one is listed as the  
3 GEC; right?

4 A. Correct.

5 Q. So do you know why CISA is listed  
6 there, why the EIP listed CISA as a major  
7 stakeholder group in the EIP?

8 MR. GARDNER: Objection, calls for  
9 speculation.

10 A. Yeah, I don't know why.

11 Q. Down at the bottom, it says: Four  
12 major stakeholder groups that collaborated with  
13 the EIP. Do you believe that CISA collaborated  
14 with the EIP?

15 A. Did we have conversations with  
16 representatives of the EIP? Yes. If that's  
17 considered collaboration then I guess we  
18 collaborated with the EIP.

19 Q. Tell me about those conversations.  
20 I know you mentioned a couple of them or a few  
21 of them, already. I take it those included a  
22 call with Alex Stamos to talk about the gap;  
23 right?

24 A. Yep.

25 Q. And it included facilitating

1 meetings between the EIP and NASED and NASS;  
2 correct?

3 A. Yes.

4 Q. And it included in some -- I take  
5 it, it included in some connection putting EIP  
6 in touch with Center For Internet Security;  
7 correct?

8 A. That's correct.

9 Q. And I take it were you kind of  
10 putting them in touch with the EI-ISAC people  
11 for the Centers For Internet Security?

12 A. I don't recall that we put them in  
13 touch with the EI-ISAC people. We put them in  
14 contact with CIS-specific people.

15 Q. And, in particular, I think you  
16 mentioned someone called Aaron; is that right?

17 A. Yes, Aaron, Aaron, as far as I'm  
18 aware, did not work for the EI-ISAC. He worked  
19 just for CIS.

20 Q. What other conversations with  
21 representatives of EIP do you recall, other than  
22 those four we just listed?

23 A. As I mentioned earlier, I believe  
24 we had some conversations when they put out  
25 public reports. If we had any questions about

1 those public reports I believe we have had a  
2 couple conversations about that.

3 **Q. Sorry, go ahead and finish.**

4 A. No, I think that's -- I think  
5 that's it, that I recall.

6 **Q. Who was involved in those**  
7 **conversations about the public reports?**

8 A. Again, it would likely be  
9 Masterson, and then there probably would have  
10 been some staff. So I don't know specifically,  
11 but there would have been other election  
12 security staff, and probably other MDM-specific  
13 team staff. But I don't recall who,  
14 specifically, it would have been. It could have  
15 shifted, you know, based on who was available,  
16 and things like that, so -- so I don't recall.

17 **Q. About how many conversations of**  
18 **that nature, relating to public reports, do you**  
19 **recall?**

20 A. To be honest, I don't recall any,  
21 specifically. I just know that we had a few.  
22 And so I -- I don't want to make up a number for  
23 you, but it was -- it was probably somewhere  
24 between two and four.

25 **Q. And were you on the two and four**

1           **conversations or did other people have them?**

2           A.     I mean, those are the ones that I  
3           recall, so those are the ones I would have been  
4           on, I don't know if there are others that other  
5           people from CISA would have been on, that I was  
6           not.

7           **Q.     Okay.  What was discussed in the --**  
8           **about their public reporting in the**  
9           **conversations you were involved in?**

10          A.     We would just ask questions about  
11          tactics and things like that, what they were  
12          seeing.

13          **Q.     What kind of contacts would they**  
14          **have?**

15          A.     They were just fairly brief  
16          conversations -- sorry -- they were just fairly  
17          brief conversations, based on blog posts.  So if  
18          we had a question about jurisdiction being  
19          targeted or a new tactic or things like that, we  
20          would just ask them kind of questions about that  
21          sort of thing.

22          **Q.     And what -- when you said tactics,**  
23          **those are kind of online tactics for spreading**  
24          **social media misinformation and disinformation?**

25          A.     Correct.  Like we were talking

1 about earlier, the coordinated inauthentic  
2 behavior. So were they using things like bots  
3 or stuff like that, kind of what was their --  
4 the technique that they were using to  
5 distribute.

6 **Q. Were people at CISA following their**  
7 **blog posts to sort of, you know, get information**  
8 **from them?**

9 MR. GARDNER: Objection, calls for  
10 speculation.

11 A. Yeah, can you specify what you mean  
12 by people?

13 **Q. Was anyone at CISA following the**  
14 **EIP's public reports?**

15 MR. GARDNER: Same objection.

16 A. I can only speak for myself. I was  
17 following the public reports.

18 **Q. Okay. How about anyone -- how**  
19 **about anyone on your team?**

20 MR. GARDNER: Same objection.

21 A. Yeah, I mean, I -- they likely  
22 were, but, you know, I couldn't say for certain.

23 **Q. And so --**

24 A. The only job requirement -- there's  
25 nobody responsible on my team, as part of their

1 job, to regularly file to the EIP reporting.

2 Q. I take it you did it, and saw some  
3 stuff you thought was interesting; is that  
4 right?

5 A. Yeah.

6 Q. And then are you the one who  
7 decided to reach out to them and ask questions  
8 about follow-up questions about stuff that they  
9 posted?

10 A. Yeah.

11 Q. And then do you remember anything  
12 specific about the tactics they flagged in their  
13 blog posts?

14 A. I don't.

15 Q. Who did you talk to at the EIP when  
16 you reached out?

17 MR. GARDNER: Objection to the form  
18 of the question.

19 A. I don't recall.

20 Q. Was it Mr. Stamos?

21 A. It could have been Alex, it could  
22 have been Renée. I forget, kind of, how they --  
23 I forget how we connected with them.

24 Q. Did you already know Alex Stamos  
25 and Renée DiResta when these conversations

1       **started happening in the summer of '20?**

2               A.    I knew Alex Stamos from previous --  
3       from when he was at Facebook.  And then, as I  
4       mentioned, Masterson and I went out to an event  
5       that Stamos hosted when he got to the Stanford  
6       Internet Observatory.  So I knew him.  Renée, I  
7       think I may have had a conversation or two with,  
8       prior, but I didn't know her as well as Alex.

9               **Q.    You say you knew him when he was at**  
10       **Facebook.  What was your interactions with him**  
11       **then?**

12              A.    He headed the team at Facebook that  
13       we did the coordination for some of the initial  
14       government industry meetings.  So if you recall  
15       back then, essentially the first meeting was  
16       back in 2018, Alex was the Facebook lead for  
17       that meeting.

18              **Q.    So he was the contact person at**  
19       **Facebook that would be in those meetings that**  
20       **involved CISA and ODNI and DOJ and the FBI?**

21              A.    Correct.

22              **Q.    I just want to flip one page in the**  
23       **report.  Up here on the screen share, do you see**  
24       **up here they have a comment that says:**  
25       **Additionally, the Countering Foreign Influence**

1 Task Force, a subcomponent of CISA, aided in the  
2 reporting process and in implementing resilience  
3 efforts to counter misinformation; do you see  
4 that sentence?

5 A. I do.

6 Q. I take it the counter -- countering  
7 and foreign influence task force is now called  
8 the MDM team that you lead; right?

9 A. Yeah, that's correct.

10 Q. Were you the leader of that team  
11 then called the CFITF in 2020?

12 A. I was.

13 Q. Do you know what the report means  
14 when it says that the CFITF, which was your  
15 team, aided in the reporting process?

16 MR. GARDNER: Objection, calls for  
17 speculation.

18 A. Yeah, I -- I don't know,  
19 specifically, what they're referencing. My  
20 assumption would be they're referencing a  
21 switchboarding we discussed earlier.

22 Q. Tell me about that switchboarding.  
23 I take it your testimony earlier was that you --  
24 you were switchboarding or routing  
25 disinformation concerns to social media



1 platforms and that there was coordination with  
2 CIS and EIP on how they should be reported;  
3 correct?

4 A. No, that's not correct.

5 Q. Okay.

6 A. So I believe what my testimony said  
7 earlier is that you would receive -- generally  
8 receive reporting through one of three ways, one  
9 of those was through the Center For Internet  
10 Security, two-fifths of that we would then  
11 forwarded to the platforms.

12 I don't recall any reporting  
13 directly coming from EIP. So generally  
14 speaking, that's, you know, adding EIP into your  
15 question I think is incorrect.

16 Q. What were the other two ways, you  
17 said there were three ways, one is you get  
18 them --

19 A. Yep.

20 Q. -- through Center for Internet  
21 Security, what are the other two?

22 A. So the other two ways, sometimes  
23 election officials would send them in to CISA  
24 central, which is CISA's kind of ops center  
25 block room type setup. And then the third way

1 was they would just send direct to a CISA  
2 employee, often -- often Matt Masterson, who had  
3 relationships with many of the election  
4 officials. So those were the principal ways we  
5 received reporting from election officials.

6 **Q. So through the CIS, kind of**  
7 **directly to -- was there a kind of e-mail**  
8 **address for reporting misinformation that CISA**  
9 **maintained?**

10 A. Not specific to misinformation. It  
11 was -- CISA central had their own e-mail  
12 address, and obviously Matt had his. We had an  
13 internal CFITF e-mail address, but I don't  
14 believe we -- we put that out for election  
15 officials to send messages to, I don't recall us  
16 doing that.

17 **Q. And then sometimes they would go to**  
18 **straight to Mr. Masterson?**

19 A. Right.

20 **Q. And then I take it you -- did you**  
21 **coordinate with CIS on what you were reporting**  
22 **to social media platforms?**

23 A. Only in the sense that we would let  
24 them know when we reported something to a  
25 platform, again, to avoid duplication or, you

1 know, most of the reporting that I recall in  
2 2020 came through CIS. And so we just wanted to  
3 let them know that we were acting on what they  
4 sent us.

5 For reporting that didn't come  
6 through CIS, we would often let them know after  
7 we had shared it with the platforms that we had  
8 shared something with the platforms for their  
9 arrangement.

10 **Q. And then I take it you said**  
11 **earlier, your understanding is that CIS was**  
12 **coordinating with EIP?**

13 A. Again, they had a relationship. I  
14 don't know how I would characterize what they  
15 were -- what they were doing with the EIP.

16 **Q. Do you know what interactions they**  
17 **had, at all, other than the ones we talked about**  
18 **between CIS and EIP?**

19 A. I mean, I can't specifically say  
20 what they were doing. They had a relationship.  
21 They shared information. I don't know kind of  
22 the extent of that or kind of what their  
23 policies and procedures were for what they were  
24 doing. So I know they were sharing stuff. I  
25 don't know what, how or when, towards the

1 questions.

2 Q. I'm going to jump ahead to page 35  
3 of this report.

4 A. 35? All right.

5 Q. That's going to be on page 53 of  
6 the PDF?

7 A. Almost there, sorry. All right.  
8 I'm on 35.

9 Q. If you look here on the last  
10 sentence before that heading on the page, it  
11 says, according to the EIP, interestingly, just  
12 one percent of tickets related to COVID-19, and  
13 less than one percent related to foreign  
14 interference; do you see that?

15 A. I do.

16 Q. Is that consistent with your  
17 understanding of the reports that you were  
18 making to social media platforms in that  
19 timeframe that only a small minority related to  
20 before and afters?

21 MR. GARDNER: Objection, lack of  
22 foundation, calls for speculation.

23 BY MR. SAUER:

24 Q. If you know.

25 A. So CISA does not do attribution.

1 We didn't do analysis of what we received from  
2 election officials. So we would not know what  
3 percentage were foreign derived.

4 Q. So you would receive reports and  
5 you would forward them onto social media  
6 platforms, you know, for consideration under  
7 their content moderation policies, without  
8 assessing whether they were originated from  
9 foreign or domestic sources?

10 A. That's correct.

11 Q. In other words, a report would come  
12 in, and you, like, didn't take steps to see  
13 whether this came from a foreign or domestic  
14 source?

15 A. Correct.

16 Q. You would just pass it along to the  
17 social media platforms?

18 A. Right.

19 Q. Are you familiar with the gateway  
20 pundit?

21 A. Am I familiar with it? Yeah.

22 Q. How do you know about it, what is  
23 the gateway pundit, on your understanding?

24 A. It's some sort of a website.

25 Q. How do you know about it?

1 A. I believe they've written some  
2 articles about CISA.

3 Q. How did that get on your radar  
4 screen?

5 A. Articles probably in our clips.

6 Q. Do you remember hearing --

7 A. I don't -- I don't --

8 Q. Go ahead.

9 A. I don't recall specifically how  
10 they got on my radar.

11 Q. Do you remember hearing of them in  
12 any other connection, other than writing  
13 articles about CISA?

14 A. I do think of the general kind of  
15 recall. Yeah, I think probably just as a  
16 general fact that it had news on it I think is  
17 probably the extent of what I know.

18 I'm sure I've just seen them, you  
19 know, in reading other stories and things like  
20 that, I don't -- I don't -- honestly, I don't  
21 know how I came to know them.

22 Q. Are you aware of anyone at CISA  
23 raising concerns that the gateway pundit might  
24 be spreading misinformation or disinformation?

25 A. No.

1 Q. I'm going to jump far down in this  
2 document to page 196.

3 A. Let me see if there's a quick way  
4 for me to get down there.

5 Q. Yeah, it's page 213 of the PDF.

6 MR. GARDNER: I think you can go  
7 here. That's a lot.

8 THE WITNESS: Sorry.

9 MR. GARDNER: Yeah, you have to  
10 scroll. All right, John, we're getting there.

11 THE WITNESS: It's two what in the  
12 PDF? I'm sorry.

13 BY MR. SAUER:

14 Q. It's page 214 of the PDF.

15 A. Okay. 196. Almost there. Sorry.

16 Okay. Yep.

17 Q. Okay. Do you see here, there's a  
18 whole section that begins: The gateway pundit  
19 interval?

20 A. I see that.

21 Q. In the first sentence of that says:  
22 The gateway pundit was among the most active  
23 spreaders of election-related misinformation in  
24 our analyses; correct?

25 A. That's what it says.

1 Q. Does that ring a bell, at all? Do  
2 you recall anyone at CISA ever raising the  
3 concern that the gateway pundit was a spreader  
4 of so-called election-related misinformation?

5 MR. GARDNER: Objection. Asked and  
6 answered.

7 BY MR. SAUER:

8 Q. Do you recall that?

9 A. Yep. As I said earlier, I don't  
10 recall any examples of that, no.

11 Q. Jump ahead to page 211. This is  
12 page 229 of the PDF.

13 A. Almost there. Okay. 211, policy.

14 Q. Yeah, chapter six.

15 A. Gotcha.

16 Q. There at the introduction, at the  
17 very beginning, it says: Platform policies  
18 establish the rules of participation in social  
19 media communities; correct?

20 A. Yes.

21 Q. It says: Recognizing the  
22 heightened rhetoric and the use of mis and  
23 disinformation during the 2020 election, all the  
24 major platforms made significant changes to  
25 election integrity policies, both as the



1        **campaigns kicked off and through the weeks after**  
2        **election day; correct?**

3            A.    Yes.

4            **Q.    And let me ask you this: Are you**  
5        **aware of social media platforms like Twitter and**  
6        **Facebook and YouTube and so forth changing their**  
7        **election integrity policies to limit**  
8        **election-related misinformation and**  
9        **disinformation during 2020?**

10           A.    I'm aware that they changed  
11        policies. I don't know -- again, I don't know  
12        that they needed mis and disinformation as their  
13        terminology, so I don't want to go there. But I  
14        do recall that they changed policies in 2020  
15        related to election security.

16           **Q.    How did you know that, at the time,**  
17        **did they report it to you?**

18           A.    They -- they did talk about some of  
19        it in our regular sync meetings. And then I  
20        believe there's some media coverage and public  
21        statements that they made about their changes.

22           **Q.    In the sync meetings, were there**  
23        **any questions on the government side? Did the**  
24        **government ask: What are you doing to change**  
25        **your policies?**

1           A.    I don't recall that. I think,  
2           generally speaking, the platforms would just  
3           talk, you know, on a regular course of the  
4           conversation they would -- that would be one of  
5           their briefing points, that they were making  
6           significant changes. But it wasn't an essential  
7           part of the conversations, generally speaking.

8           **Q.    Were you aware of anyone in the**  
9           **federal government kind of asking or encouraging**  
10          **them to change their content moderation policies**  
11          **to address election integrity?**

12          A.    Not that I'm aware of, no.

13          **Q.    Do you recall, was it placed on the**  
14          **agenda for the sync meetings?**

15          A.    Was what placed on the agenda?

16          **Q.    Changes in content moderation**  
17          **policies.**

18          A.    Not that I recall.

19          **Q.    Do you know how it came up in those**  
20          **meetings?**

21          A.    Again, I think, you know, part of  
22          the meetings were generally different  
23          participants providing updates on what they were  
24          doing relating to election security. And my  
25          recollection is, is that platforms might raise

1 those sorts of things during that portion of the  
2 agenda.

3 **Q. Did they ever separately e-mail you**  
4 **to notify you of a content policy update?**

5 A. Not that I recall, though it's  
6 certainly possible. You know, I would get press  
7 releases that they would put out sometimes, they  
8 would forward to me. But I don't recall  
9 specific e-mail on that.

10 **Q. Do you know whether anyone at the**  
11 **Center For Internet Security discussed content**  
12 **policy changes with the social media platforms?**

13 A. I don't.

14 **Q. Do you know whether anybody at CISA**  
15 **did so during the 2020 election cycle?**

16 A. Not that I'm aware of, no.

17 **Q. How about Mr. Masterson?**

18 A. Not that I'm aware of.

19 **Q. What was Mr. Masterson's title or**  
20 **what was his role at CISA during this timeframe**  
21 **in 2020?**

22 A. He was the senior -- I don't know  
23 what his exact title was, but he was a senior  
24 election security person at CISA.

25 **Q. So did you report to him when you**

1           **were the head the countering foreign influence**  
2           **task force?**

3                   A.    No.  Matt was what I call a  
4           political appointee, so for organizational  
5           reasons I reported up to Geoff and Geoff  
6           reported to a normal chain of command.  So there  
7           was something weird about Matt being a political  
8           appointee and where he could sit in the org  
9           chart, so none of us technically reported up to  
10          him.

11                   Q.    So he was -- but he was -- as a  
12          **political appointee is higher than you in the**  
13          **org chart?**

14                   A.    Yeah.

15                   Q.    Okay.  And did you coordinate with  
16          **him on the sort of -- sort of disinformation and**  
17          **misinformation related activities that CISA was**  
18          **engaged in, in 2020?**

19                   MR. GARDNER:  Objection, vague.

20                   A.    Yeah, could you be a little more  
21          clear in what you're asking, please?

22                   Q.    Well, did you work with Matt  
23          **Masterson on election disinformation and**  
24          **misinformation related issues in 2020?**

25                   A.    Yes.

1 Q. Okay. What sort of work did you do  
2 with him?

3 A. Again, a majority of our work, as I  
4 mentioned earlier, was resilience building, so  
5 trying to develop products, public education,  
6 public awareness, product to help election  
7 officials, those sort of things. And then I  
8 would have discussed with him -- he would have  
9 been familiar with the switchboarding work that  
10 we were doing.

11 Q. Did he participate in the  
12 switchboarding work?

13 A. Not beyond when he would receive  
14 e-mails, he forwarded them to us.

15 Q. Well, he would send them to you to  
16 be switchboarded, so to speak?

17 A. Yeah, I mean, he would send them to  
18 me or the team e-mail address.

19 Q. Oh, and you mentioned earlier that  
20 he had close relationships with social media  
21 platforms?

22 A. No, I don't think I ever said that.  
23 He had close relationships with election  
24 officials.

25 Q. Oh, okay. Did you also mention

1       **that he was in -- he had contacts with social**  
2       **media platforms?**

3               A.     Again, he would have participated  
4     in the sync meetings that I talked about, the  
5     government industry syncs. If we had a briefing  
6     or something at other meetings he would likely  
7     participate. Those are the only communications  
8     I'm aware of, but he may have had others. I'm  
9     not sure.

10              **Q.     Are you aware of anyone at the**  
11     **Election Integrity Partnership communicating**  
12     **with the social media platforms about changing**  
13     **their policies to, you know, kind of restrict**  
14     **election-related misinformation?**

15              A.     I am not, no.

16              **Q.     Is that something, that idea of**  
17     **advocating to the social media platforms to**  
18     **adopt more restrictive policies on**  
19     **election-related misinformation, is that**  
20     **something that's -- that you recall coming up in**  
21     **any meetings or discussions you had in 2020?**

22              A.     So did we ever have -- so one, if  
23     you can clarify who the meetings were with, that  
24     you're asking about.

25              **Q.     I'm asking --**

1           A.    Or the general -- did anyone at  
2           CISA meet to discuss changes in platform policy?  
3           To the best of my recollection, the answer is  
4           no, we never meant to discuss asking the  
5           platforms to make any changes to their policies.

6           **Q.    Do you recall -- I take it that was**  
7           **a response as to internal meetings, are you**  
8           **aware of any meetings with anyone external to**  
9           **CISA to discuss, you know, changes in platform**  
10          **policies?**

11          A.    I'm not aware of any external  
12          meetings along those lines.

13          **Q.    Do you recall any communications of**  
14          **any kind that related to that in 2020?**

15          A.    Any communications that related to  
16          what? To -- to platforms changing their  
17          policies? Any communications -- with -- I mean,  
18          that's a very broad -- I mean, it's possible  
19          that somebody at CISA, along the way, had a  
20          conversation about that, but I don't recall any  
21          specific conversations where we sat down to talk  
22          specifically about that. I don't -- I don't  
23          recall any of that. It's a very broad answer,  
24          so I don't want to say definitively that nobody  
25          at CISA ever had any conversations in 2020 about

1 policy changes.

2 Q. How about you, do you recall  
3 communicating with anyone outside of CISA about  
4 social media platform policy changes in 2020?

5 A. I don't. I don't.

6 Q. Have you ever heard of the Virality  
7 Project?

8 A. I have.

9 Q. What is the Virality Project?

10 A. My understanding, it was Stanford's  
11 attempt to mimic the EIP for COVID.

12 Q. How do you know about that?

13 A. Good question. I believe they sent  
14 me some of their public reports.

15 Q. The Virality Project did?

16 A. Yes.

17 Q. Who -- who would have sent those to  
18 you? Was it the same people involved in -- same  
19 people involved in the Election Integrity  
20 Partnership?

21 A. I think Alex was involved, and I  
22 believe Renée was involved. I don't know if the  
23 rest were similar or not. I don't recall who  
24 was sending it, the exact individual who was  
25 forwarding me their reports.



1 Q. Was that --

2 A. And to be honest, I'm not sure if  
3 they sent them directly to me or if they went to  
4 somebody else in government who forwarded it to  
5 me.

6 Q. Okay. Was there -- did you have an  
7 oral conversation with anyone associated with  
8 the Virality Project about what they do?

9 A. Not specifically about what they  
10 do, but I did have some conversations where they  
11 were asking us for -- asking me, not us -- for  
12 any connections I had with HHS or CDC.

13 Q. And did you provide them with  
14 connections?

15 A. I did not.

16 Q. What did you -- what did you say in  
17 that conversation?

18 A. I don't recall that I had any --  
19 any relevant points of contacts to provide them.

20 Q. Did you have any other  
21 conversations with them relating to the Virality  
22 Project?

23 A. Not -- not substantial. I'm trying  
24 to think. I mean, I -- most of that work took  
25 place when I was over at the National Security

1 Council, so I had substantially less  
2 communication.

3 But I believe there were some  
4 informal kind of not work conversations that I  
5 may have had with Alex, in particular, and maybe  
6 Renée, as well.

7 **Q. You believe when you were detailed**  
8 **to the National Security Council you had**  
9 **conversations with Alex Stamos and Renée DiResta**  
10 **about the Virality Project?**

11 A. Just in the sense that it was  
12 something that they were doing, and that was  
13 when I think Alex asked if I had any contacts is  
14 when I was at the National Security Council.

15 **Q. Did you and Alex discuss anything**  
16 **else about it? And let me ask you this: Did he**  
17 **give you any kind of overview what they planned**  
18 **to do in the Virality Project?**

19 A. Not beyond that it was similar to  
20 what they did with the -- with the EIP, that was  
21 the extent. We didn't get into any details or  
22 anything like that.

23 **Q. And he asked you for contacts at --**  
24 **at kind of federal kind of health agencies?**

25 A. Yeah, that's my recollection of

1 what he was asking for.

2 **Q. And did you have any other**  
3 **discussions with him that related to Virality**  
4 **Project?**

5 A. Not that I recall. I don't know  
6 that we ever got briefed on their work, so I  
7 don't think there was anything like that. So I  
8 think to the extent was, you know, that  
9 conversation about that, and then, like I said,  
10 I believe I received some of their reports, the  
11 public reports.

12 **Q. And you say either they or someone**  
13 **within government forwarded you with their**  
14 **public reports?**

15 A. Right, yeah, I don't recall exactly  
16 how I got them. I think it was from -- from the  
17 Virality Project, itself, but I'm not a hundred  
18 percent certain of that.

19 **Q. And let me ask you this: Was CISA**  
20 **active in -- in -- or take any activities to**  
21 **follow or address information -- misinformation**  
22 **relating to COVID-19?**

23 A. I believe we did at least one  
24 product for our critical infrastructure  
25 stakeholders related to COVID-19.

1 Q. How about --

2 A. It should be on our -- sorry.

3 It should be on our public website.

4 Q. How about switchboarding, did CISA  
5 do any switchboarding related to COVID-19  
6 misinformation concerns?

7 A. No.

8 Q. And again, the switchboarding  
9 that -- when I use that term I'm using your term  
10 for kind of routing disinformation concerns and  
11 misinformation concerns to the social media  
12 platforms; correct?

13 A. Correct, yeah, as far as I'm aware  
14 there was no -- there was none of that occurred  
15 related to COVID.

16 MR. SAUER: I'm going to pull up  
17 Exhibit 2 on the screen share, which has also  
18 been e-mailed to you, which is the Virality  
19 Project's public reporter.

20 (Exhibit No. 2 was marked for  
21 identification.)

22 MR. GARDNER: Hold on one second,  
23 John.

24 MR. SAUER: Which is the Virality  
25 Project's public report, Virality,

1 V-i-r-a-l-i-t-y.

2 MR. GARDNER: Yeah, hold on, John.

3 Hold on, John. Hold on. Got it.

4 BY MR. SAUER:

5 Q. You mentioned -- before we turn to  
6 the document, you mentioned that you had  
7 conversations with Alex Stamos and Renée DiResta  
8 about the Virality Project. What were the  
9 nature of the conversations with Renée DiResta?

10 A. They were at the same time as the  
11 conversations with Alex. I believe it was  
12 similar content. And I don't -- it wasn't a  
13 lengthy conversation, it was just, hey, we're  
14 doing something, I believe.

15 Q. Mm-hmm. Did she ask you for any  
16 context or anything like that?

17 A. I'm sorry, could you repeat that?

18 Q. Did she ask you for any context or  
19 anything like that?

20 A. Not that I recall, but I think she  
21 was with Alex when we had that conversation.

22 Q. So you believe it was the same  
23 conversation with Alex and Renée happened at the  
24 same time?

25 A. Yeah, I believe we were having a

1 meeting, they were briefing us about -- so I  
2 think this was connected to when I got the brief  
3 on the report, the election report, when I was  
4 at the White House. I think that's when they  
5 mentioned that they were going to potentially do  
6 something similar around COVID, and asked if we  
7 had any contacts.

8 **Q. And did you -- and I take it you**  
9 **said earlier you didn't have any contacts;**  
10 **right?**

11 A. Yeah, I didn't have any good  
12 contacts at CDC or HHS.

13 **Q. Did you ask anyone else in**  
14 **government if they had contacts that would be**  
15 **useful to them?**

16 A. I don't recall doing that, so I  
17 don't think so.

18 **Q. Did you notify people at the White**  
19 **House about, you know, the briefing you got from**  
20 **them or the information you got from them?**

21 A. So I'm sure I talked to my  
22 supervisor about the election briefing. I may  
23 have mentioned, although I don't recall if I did  
24 or not, that they were going to do something  
25 similar for -- for COVID.

1 Q. What did you report back about the  
2 election briefing? I take it that's the long  
3 fuse report from the Election Integrity Project  
4 right, or partnership; right?

5 A. Yeah, just to the extent we -- just  
6 in general, we met with them kind of shared kind  
7 of their lessons learned, kind of what some of  
8 their big takeaways were. I don't recall what  
9 the specifics were. It was a brief kind of  
10 conversation in passing.

11 Q. Who was your supervisor at that  
12 time?

13 A. Kaitlin Gegovich (phonetic).

14 Q. Looking at the Virality Project  
15 report, skipping ahead to page 4 of the report?

16 A. 4, 4, or Roman numeral four?

17 Q. Regular four.

18 A. Gotcha.

19 Q. Is there's recommendations --

20 A. Okay. Okay.

21 Q. Is there a recommendation here to  
22 implement misinformation and disinformation  
23 center of excellence housed within the cyber  
24 security infrastructure security agency; do you  
25 see that?

1 A. I do.

2 Q. So Stanford recommends that the  
3 government create a misinformation and  
4 disinformation center of excellence housed  
5 within CISA; correct?

6 MR. GARDNER: Objection. He said  
7 it calls for speculation.

8 A. That's what the sentence says.

9 Q. Did they ever discuss --

10 A. What they meant by that, I don't  
11 know what they meant.

12 Q. Did they ever -- did Alex Stamos or  
13 Renée DiResta ever discuss that with you, you  
14 know, having CISA take on a new and more  
15 formalized roll with respect to misinformation  
16 and disinformation?

17 A. Not that I recall. I don't think I  
18 was ever briefed on this report, so I don't  
19 recall having that conversation.

20 Q. Do you know of anyone -- they  
21 talked to anyone else at CISA about that?

22 A. I don't know. I don't know.

23 Q. By the time of this report, in  
24 2021, Matt Masterson was actually working for  
25 the Stanford Internet Observatory; correct?



1 A. I believe so, yeah.

2 Q. **Have you ever read this report**  
3 **before?**

4 A. I think I read a little bit of it,  
5 but I don't think I read the whole -- I don't  
6 recall. I haven't read the whole thing. I  
7 shouldn't say I don't recall. I haven't read  
8 the whole thing.

9 Q. **Do you know when you read it?**

10 A. I don't.

11 Q. **Do you know why you read it?**

12 A. I mean, I would read it, generally  
13 speaking, I'm interested in understanding what  
14 researchers find related to mis, dis and  
15 mal-information.

16 Q. **I'm sorry, relating to what?**

17 A. What researchers find, understand,  
18 what they're learning relating to mis, dis and  
19 mal-information.

20 Q. **And did you have any takeaways from**  
21 **this report, that informed your work at the MDM**  
22 **team?**

23 A. I don't think there's anything  
24 specific that we took from this, from a product  
25 standpoint or anything like that.

1 Q. Do you know how -- do you know how  
2 the Virality Project tracked, you know,  
3 misinformation narratives about COVID vaccines  
4 on social media?

5 A. I don't.

6 Q. I'm going to jump ahead to page 30  
7 of the report, very usefully that's also page 30  
8 of the PDF.

9 A. Making things easier.

10 Q. I think they learned a lesson after  
11 the first report.

12 A. Yeah.

13 Q. Reference here to your --

14 A. Okay. Got you.

15 Q. There's a reference here to tiered  
16 ticket analysis, it says: Their analysis  
17 consisted of lateral -- lateral research that  
18 used Crowd Tangle and Google searches to assess  
19 the spread of the incident or content and so  
20 forth; do you see that?

21 A. I do.

22 Q. What Crowd Tangle is?

23 A. I believe Crowd Tangle was a  
24 Facebook-owned social media monitoring service.

25 Q. And is that something that's

1 available to the public? Can the public kind of  
2 subscribe to Crowd Tangle?

3 MR. GARDNER: Objection.

4 BY MR. SAUER:

5 Q. Or is it kind of a --

6 MR. GARDNER: Objection. Sorry.

7 Sorry, thought you were done, John, please, are  
8 you done?

9 MR. SAUER: Yeah.

10 MR. GARDNER: Sorry, objection,  
11 lack of foundation.

12 A. So I don't know -- I don't know the  
13 nature of Crowd Tangle, if it's publicly  
14 available or not.

15 Q. Have you ever heard of it before?

16 A. I have.

17 Q. In what connection have you heard  
18 of it?

19 A. Just talking, you know, in the  
20 general, mis, dis, mal-information research  
21 community, I know it's a tool that some  
22 researchers use.

23 Q. Okay. Next page of the report,  
24 there's a reference to collecting video --  
25 there's a reference to -- it says: The

1 engagement data or video view data for links  
2 associated with each ticket is collected  
3 differently depending on the social media  
4 platform in question, colon; do you see that?

5 A. I do.

6 Q. It talks about how Facebook and  
7 Instagram, they used Crowd Tangle API; right?

8 A. I see that, yeah.

9 Q. What is -- do you know what API  
10 stands for?

11 A. I don't.

12 Q. Okay. Same question, then, as to  
13 Twitter, it says Twitter API, YouTube, API, do  
14 you know what API refers to?

15 A. I --

16 MR. GARDNER: Objection, asked and  
17 answered.

18 A. Yeah, I don't know, that's a little  
19 above my technical knowledge.

20 Q. Let's jump ahead to page 143.

21 A. Okay.

22 Q. Okay. Here under: Maintain clear  
23 channels of communication across all levels of  
24 government; do you see that?

25 A. I do.

1 Q. And then there in this sentence it  
2 says -- or sorry, in this paragraph -- it says:  
3 For example, as voting-related mis and  
4 disinformation arose in the 2020 presidential  
5 election, the Election Infrastructure  
6 Information Sharing and Analysis Center, EI-ISAC  
7 served a critical role in sharing information in  
8 the Election Integrity Partnership in pushing  
9 its rapid response analysis back out to election  
10 stakeholders across the states; right?

11 A. That's what the sentence says,  
12 yeah.

13 Q. And I take it, we asked you this  
14 before, but are you aware of the EI-ISAC  
15 sharing -- serving a critical role in sharing  
16 information with the EIP during 2020?

17 A. I -- I'm not. My understanding and  
18 recollection it was Center For Internet  
19 Security, it's of course possible that the  
20 Stanford folks are conflating the EI-ISAC with  
21 the Center For Internet Security, kind of we  
22 talked about earlier, they're kind of part of  
23 the same organization, but I'm not aware of  
24 those sorts of direct communications with  
25 EI-ISAC.

1 Q. What is the difference between the  
2 EI-ISAC and the CIS? My understanding was that  
3 the CIS was a non-profit, and EI-ISAC is kind of  
4 like a program that it runs, that allows for  
5 information sharing among state and local  
6 election officials, is that the distinction of  
7 what's the difference?

8 MR. GARDNER: Objection, form.

9 BY MR. SAUER:

10 Q. You may answer.

11 A. What's the difference between what,  
12 CIS and EI-ISAC.

13 Q. Yeah, what's the distinction  
14 between them.

15 A. I mean, I don't -- to be honest, I  
16 don't fully know what the distinction is, my  
17 understanding is it's roughly, as you kind of  
18 stated it, right, is CIS is an umbrella  
19 organization that has organizations underneath  
20 it. I don't know what the operating  
21 relationship is between the EI-ISAC and CIS. If  
22 it's a direct line, I just don't know how they  
23 operate that way.

24 But my understanding is that the  
25 CIS has its own staff, and that those staff and

1 their own funding, and that that staff and  
2 funding is what supported the 2020 election  
3 switchboarding work.

4 Q. So, in other words, you think the  
5 CIS was -- was switchboarding to EIP during  
6 2020?

7 A. I'm not sure that's what I said. I  
8 mean, the relationship that I understood was  
9 between CIS and EIP, what specifically they were  
10 doing as part of that relationship I'm not --  
11 again, I don't necessarily want to speak to,  
12 because I'm not 100 percent sure how it worked.

13 Q. Well, is the EI-ISAC kind of a  
14 vehicle in which CIS receives reports of  
15 misinformation and disinformation from state and  
16 local election officials?

17 MR. GARDNER: Objection, lack of  
18 foundation, calls for speculation.

19 A. Yeah, I don't know how -- how the  
20 EI-ISAC played in this switchboarding role.

21 Q. Down here at the bottom of the same  
22 page there's another reference to the  
23 recommendations to implement a misinformation  
24 and disinformation center of excellence housed  
25 within the federal government; correct?

1 A. Yeah.

2 Q. And that there in that paragraph it  
3 specifically recommends that it be housed within  
4 the federal government at CISA; correct? See  
5 where I've highlighted?

6 A. Yeah, I'm just reading that now.  
7 Yeah, that's what the sentence  
8 says, yeah.

9 Q. Do you have any recollection -- let  
10 me ask you this: I think you testified earlier  
11 you don't remember discussing that  
12 recommendation with anyone; correct?

13 A. Correct.

14 Q. Okay. How about any discussions of  
15 changing or increasing CISA's role in -- in kind  
16 of tracking or monitoring online dis and  
17 misinformation?

18 MR. GARDNER: Objection to the  
19 extent that answers calls for the disclosure of  
20 information, subject to the local process  
21 privilege. I would instruct the witness not to  
22 answer. To the extent that you can answer that  
23 without disclosing information related to the  
24 privilege you can do so.

25 THE WITNESS: I'm sorry, can you



1 repeat the question, just to make sure I  
2 understand it.

3 MR. SAUER: Let's break it down.

4 BY MR. SAUER:

5 Q. Do you recall any discussions with  
6 anyone outside of CISA about expanding CISA's  
7 role in addressing misinformation and  
8 disinformation concerns on social media?

9 A. CISA's role, expanding CISA's role,  
10 yeah. Yes.

11 Q. Okay. What conversations do you  
12 remember about that?

13 A. So we were piloting a capability  
14 that would allow us to monitor narratives  
15 online.

16 Q. Now, when was this piloted?

17 A. I believe it was -- we did one  
18 short pilot, I believe, in summer 2020, so I  
19 believe it was all 2020.

20 Q. What -- what -- what sort of  
21 pilighting -- can you explain what you mean by  
22 pilighting -- I'm sorry -- piloting something to  
23 track mis and disinformation online?

24 A. So it wasn't necessarily to track,  
25 it was to understand the information

1 environment, what narratives were -- were kind  
2 of perking up. The piloting was, as I'm sure  
3 you're aware, there was extensive -- extensive  
4 privacy rules around that sort of work, and so  
5 it was just kind of piloting it to see if it  
6 would work, if it did what we wanted it to do.

7 In particular, we were trying to  
8 predict the likely impact of narratives on  
9 stakeholders. And so we weren't sure if the  
10 predictive activity that we were doing actually  
11 worked, so we wanted to test that, and then we  
12 wanted to just get a sense of the privacy and  
13 other kind of rules that might be in play and if  
14 it's something that we could -- we could do.

15 **Q. What exactly was the pilot? I**  
16 **mean, what -- what -- did you have a computer**  
17 **program that would, you know, go out and track**  
18 **what people were saying on social media? What**  
19 **exactly was the pilot? I don't understand.**

20 MR. GARDNER: I'll object on the  
21 grounds that that calls for disclosure of  
22 information subject to deliberative process  
23 privilege. I instruct the witness not to  
24 answer.

25 MR. SAUER: Yeah, the deliberative

1 process privilege only applies when there is no  
2 indication of any government wrongdoing. Our  
3 court has already found that there's at least a  
4 substantial concern that there were significant  
5 first amendment violations, here, so I ask you  
6 to withdraw the objection.

7 MR. GARDNER: I understand your  
8 position and I decline your invitation.

9 BY MR. SAUER:

10 Q. Are you declining to answer the  
11 question, sir?

12 A. Yes.

13 Q. So in that case, can you kind of  
14 explain more generally what this pilot project  
15 involved in 2020, to track social media on the  
16 internet?

17 MR. GARDNER: To the extent that  
18 that calls for the disclosure of information  
19 subject to the deliberative process privilege I  
20 instruct the witness not to answer.

21 To the extent that you can answer  
22 that question at a high level of generality, you  
23 may do so.

24 A. Yeah, so as I mentioned, our  
25 mission is to build the variance to MDM

1 targeting critical infrastructure.

2 So essentially what we were trying  
3 to understand is if we could predict the likely  
4 impact of MDM narrative in terms of increasing  
5 risks to critical infrastructure by a better  
6 understanding the information environment, so  
7 the pilot was essentially trying to test that  
8 theory out.

9 **Q. Yeah, kind of, again, at a high**  
10 **level of generality, how do you test that theory**  
11 **out?**

12 A. So the predictive model essentially  
13 was to say -- say you had an image, it would  
14 pull particular components of an image out and  
15 based on -- I don't want to get too -- I don't  
16 know that I understand the black box that they  
17 used all that well, if I were trying to test it,  
18 but there was a methodology that they used to do  
19 that, and so we were just trying to see if that  
20 methodology, in fact, worked from a  
21 disinformation standpoint.

22 **Q. When you say: They, who's they?**  
23 **Is this people at CISA or is there a contractor**  
24 **that created a product?**

25 A. It was a contractor.

1 Q. What contractor?

2 A. I believe the company was Limbik.

3 Q. Sorry, can you spell that?

4 A. L-i-m-b-i-k.

5 And then there was a separate  
6 pilot, that's more generically around  
7 situational awareness of potential narratives  
8 online, that didn't feed into the -- into the  
9 predictive modeling.

10 Q. Was that a Limbik product, too,  
11 that second pilot?

12 A. No, that was a -- that was a  
13 different contractor, and I forget who it was.

14 Q. Did either of these pilots ever get  
15 any actual programming, something that you used?

16 A. No. The rules we operated the  
17 pilot on was that none of it could be used for  
18 operational purposes, because there's privacy  
19 requirements around that. And so essentially we  
20 were just using it for internal deliberations in  
21 terms of if the -- if the tools were helpful or  
22 not.

23 Q. Did you conclude that they were  
24 helpful?

25 MR. GARDNER: Object on the grounds

1 of deliberative process privilege. I instruct  
2 the witness not to answer.

3 MR. SAUER: To be clear, I'm asking  
4 for the conclusion, not the deliberation.

5 BY MR. SAUER:

6 Q. Did you conclude that they would be  
7 useful?

8 MR. GARDNER: Same objections, same  
9 instructions.

10 THE WITNESS: Yeah, I'm not going  
11 to answer.

12 MR. SAUER: I've e-mailed around  
13 Exhibit 9.

14 (Exhibit No. 9 was marked for  
15 identification.)

16 BY MR. SAUER:

17 Q. And if you have a minute to look at  
18 it, I'm also putting on the screen share, it's a  
19 collection of e-mails from October of 2020,  
20 produced by the government, involving CISA. And  
21 I think they relate to the switchboarding you  
22 testified there about earlier.

23 Do you see the -- the document?

24 A. I do.

25 Q. Just look here on the first page,

1       there's an e-mail, if you look here, kind of on  
2       Thursday, October 1st, at 4:23 p.m., it shows  
3       misinformation reports sending an e-mail to you,  
4       to CISA central, which I think you mentioned  
5       earlier, to CFITF e-mail address, and -- and  
6       misinformation reports; do you see that?

7               A.     I do.

8               Q.     And this is a -- I take it, some  
9       report that relates to misinformation in social  
10      media from CIS; correct?

11              A.     Let me just scroll to the beginning  
12      of the e-mail chain.

13              Yeah, this is a report I received  
14      from CIS.

15              Q.     And when CIS e-mailed you this  
16      report, if you look here, towards the top or  
17      right in the middle of the first page, CIS --  
18      first of all, it's signed by Walter Oberes and  
19      Aaron Wilson; correct?

20              A.     Yeah.

21              Q.     And that Aaron, is that the Aaron  
22      you talked about earlier, as your CIS contact?

23              A.     It is, correct.

24              Q.     And how about -- who's Walter  
25      Oberes?

1 A. I don't know.

2 Q. Okay. And he -- they say:

3 Brian -- referring to you -- we know many are  
4 already aware of this case, but the impact seems  
5 to be escalating. Our hope is the platforms can  
6 do more to take down the misinformation;  
7 correct?

8 A. That's what this says, correct.

9 Q. And then it goes on to say: The  
10 EIP has been tracking this spread under ticket  
11 EIP-243, and has more examples; correct?

12 A. Correct.

13 Q. Did they commonly tell you when the  
14 EIP was tracking online misinformation, as well  
15 as CIS?

16 A. I don't think that was common, no.

17 Q. Okay. Were you aware, at the time,  
18 of what an EIP ticket was?

19 A. I understood that EIP was using a  
20 ticketing system. That's the extent of it, so  
21 that's what I assumed it was.

22 Q. And how did you know that?

23 A. That they were using a ticketing  
24 system?

25 Q. Yeah.



1           A.     So as I mentioned earlier, we did  
2     get some briefs from them when they were setting  
3     things up, to let us know how they would work,  
4     and there was mention of a ticketing system  
5     during that, those conversations.

6           **Q.     When you received this report you**  
7     **forwarded it onto Facebook, correct, directly**  
8     **above?**

9           A.     I did.

10          **Q.     And you said --**

11          A.     Correct.

12          **Q.     And you said: This is not**  
13     **Facebook-related reporting, but thought it would**  
14     **be of interest to your team; right?**

15          A.     Right.

16          **Q.     Why did you forward it onto**  
17     **Facebook if it appears to relate to tweets or**  
18     **Twitter, as opposed to Facebook?**

19          A.     Well, it related to Twitter and I  
20     believe YouTube, if I'm reading this correctly.

21          **Q.     Yeah, why did you forward it onto**  
22     **Facebook?**

23          A.     There's a lot of ways that people  
24     generate traffic to YouTube, in particular, but  
25     Twitter, as well, is by posting it across

1 platforms.

2 So something like this, it would  
3 sometimes share across other platforms that we  
4 thought there might be -- it might be relevant  
5 content showing up on their platforms.

6 Q. In other words, if the  
7 disinformation or misinformation might be  
8 spreading to other platforms you would notify  
9 not just the platform reported, but other  
10 platforms, as well, so that they could be aware  
11 of this content; is that what you did?

12 A. Yeah. So if I'm reading this  
13 correctly, it sounds like it literally jumped  
14 platforms. So maybe I'm misreading. And so,  
15 yeah, sometimes we would just -- we would share.

16 Q. When you say: We would share, you  
17 mean you would share it with other platforms  
18 than the one that was currently hosting the  
19 reported content?

20 A. Correct.

21 Q. Okay. Just scrolling down a few  
22 pages, there a page with a Bates number 9676 at  
23 the bottom.

24 A. 9676.

25 Q. It's page 7 of the PDF.



1 answered. You can answer.

2 A. I wouldn't say it was a common  
3 practice, but we did do it period -- do it  
4 periodically.

5 Q. Let me jump ahead to Bates number  
6 8356.

7 A. Which PDF page is that?

8 Q. That looks like it's going to be  
9 page 12 of the PDF.

10 A. Okay. All right. Just so you  
11 know, for the e-mail, the PDF page numbers are  
12 going to be a lot more helpful.

13 Q. Sure.

14 A. So 8357, is that what I'm looking  
15 at?

16 Q. 56, I think it's the page before.

17 A. Oh, the one above? I got you.

18 Q. So, yeah, and I think this still  
19 relates to the same ticket; right? If you look  
20 at the middle of the page, you're still dealing  
21 with the same report from CIS that has that same  
22 EIP ticket number; correct?

23 A. Yeah, it appears correct.

24 Q. And this one you passed this onto  
25 Twitter; right?

1 A. Mm-hmm.

2 Q. And that was the platform that was  
3 directly affected; right?

4 A. Correct.

5 Q. And then talking to Twitter, at the  
6 very top, there, you said, you know, good  
7 afternoon, suspect you are -- you all are  
8 already aware of these issues, we wanted to pass  
9 along this reporting from Sonoma County,  
10 California, to see if there's anything you can  
11 share on how you're approaching; right?

12 A. Mm-hmm.

13 Q. Is that -- sorry, can you answer it  
14 with a yes or no?

15 A. Oh, I'm sorry.

16 Yes.

17 Q. Is that something you did when you  
18 were serving the switchboarding function was ask  
19 the social media platforms to report back how  
20 they had addressed the contents reported?

21 A. Generally we would do that if the  
22 election official asked.

23 Q. Why did you do that?

24 A. Well, the -- the election official  
25 reported something, they just wanted to know if

1 a decision was made often, not often, sometimes.

2 And so if the platform was open to  
3 sharing if they had made a decision or not, we  
4 would just push that back to the election  
5 officials so they were aware --

6 Q. So --

7 A. -- of where the platform landed.

8 Q. So CISA would, if the state or  
9 local official wanted to know, you know, whether  
10 the reported misinformation had been actioned in  
11 some way, CISA would ask the social media  
12 platform to report that back, and then CISA  
13 would relay that to the social media -- sorry --  
14 to the state or local official; is that right?

15 A. Yeah, we did that periodically,  
16 where we would ask if the decision was made and  
17 if we can share back.

18 Q. Did you do --

19 A. The platforms got better, along the  
20 way, of communicating directly with the election  
21 officials, themselves.

22 Q. Sometimes they would report back  
23 directly, later in the process, especially?

24 A. Yeah, I believe it got better kind  
25 of as time went on.

1 Q. Did you do anything else with that  
2 information, about whether and how the reported  
3 misinformation had been actioned by the social  
4 media platform?

5 A. Did we do anything else with it?

6 No. No. I mean, if it came to CIS  
7 we would push the response from the platform  
8 back up to CIS. If the information we received  
9 from the election official came direct to us we  
10 would push that back, just back to the election  
11 official.

12 Q. How about anyone else, would anyone  
13 else be notified how they acted?

14 A. I think we may have put a notation  
15 in the tracking spreadsheet we kept, if a  
16 platform said something returned. But that was  
17 an internal set of documents that would go to --  
18 normally our attorneys, the privacy folks, would  
19 let you see the tracking list review,  
20 periodically.

21 Q. So there was an internal  
22 spreadsheet created by CISA to track these  
23 reports?

24 A. Yes.

25 Q. And did you enter, you know, all of

1       **your switchboarding activity reports into that**  
2       **spreadsheet?**

3               A.     Yeah, we did the best we could to  
4       make sure everything was captured in there.

5               **Q.     Does that spreadsheet still exist?**

6               A.     I believe -- I would assume so.

7               **Q.     Who else -- or who would enter the**  
8       **information in this spreadsheet?**

9               A.     So the MDM team took shifts, in  
10       terms of receiving and doing -- like I said, it  
11       was very resource intensive for us, and so other  
12       members of the MDM team would have asserted  
13       stuff in there, as well, if it was their shifts.

14              **Q.     Who would have -- who took shifts,**  
15       **other than you?**

16              A.     So back then it would have been  
17       myself, Chad, Rob, from that org chart, sorry,  
18       Rob Schaul, Chad Josiah, who else was doing it  
19       back then, myself, Alex Zaheer, an intern, which  
20       I'm not going to name, and I think that was it.

21              **Q.     Let me see if I caught all --**

22              A.     I think that was it.

23              **Q.     Let me see if I caught all those**  
24       **e-mails, Chad Josiah did that?**

25              A.     Mm-hmm.



1 Q. And then I think you said Rob  
2 Schaul did that, S-c-h-a-u-l; corrects?

3 A. Correct, and then Alex Zaheer, who  
4 also should be on the org chart.

5 Q. How do you spell letter name?

6 A. His name, Alex, A-l-e-x,  
7 Z-a-h-e-e-r.

8 Q. Okay. Anyone else?

9 A. There's an intern.

10 Q. Can you name the intern, please?

11 A. No, I'm not going to name the  
12 intern.

13 Q. Are you refusing to answer that  
14 question without an instruction, again?

15 A. Yes.

16 Q. Okay. Anyone else?

17 A. I feel like there was, but I'm  
18 forgetting names, right now. But those would  
19 have been the principal -- oh, John Stafford,  
20 sorry.

21 Q. What's his role at CISA?

22 A. He is not at CISA any longer. He  
23 left sometime in 2021.

24 Q. Okay. What was his role?

25 A. He was an analyst by -- like the

1 others.

2 Q. And would all those people be  
3 involved in e-mails like the ones we're looking  
4 at here in October 9 -- sorry -- in Exhibit 9,  
5 where word would come in from, you know, CIS or  
6 somebody like that, they would forward it onto a  
7 social media platform?

8 A. Yeah, so they would -- if -- if  
9 they received something, they would play that  
10 switchboard role and they would forward it to  
11 the platforms.

12 Q. And then would they, like you,  
13 report back sometimes to CIS or whatever  
14 reporter on how things had been actioned?

15 A. I don't recall if they did that or  
16 not. If the -- if the platform sent something  
17 back on their own, which sometimes happened, as  
18 well, they would report that. I don't know that  
19 they did anything beyond that.

20 Q. Did any of them communicate with  
21 anyone at the Election Integrity Partnership?

22 A. Well, the intern, I believe, worked  
23 both, although, when he was on duty, he was only  
24 working for us. Beyond that, I don't -- I don't  
25 know. I don't know that we would have

1       conversations, not about the switchboarding, I  
2       wouldn't think.

3               **Q.    You say the intern worked both, you**  
4       **mean the intern part of the time was working for**  
5       **CISA and part of the time was working for EIP?**

6               A.    So my understanding -- so the  
7       intern was a Stanford student, so he worked part  
8       time for us.  On election day, when he would  
9       have been on the agenda, he was just working for  
10      us.

11              And my understanding is he also did  
12      some work for the Stanford Internet Observatory.  
13      I don't know what that work entailed, if it was  
14      EIP-specific or not.  But yeah, he was -- he did  
15      do some stuff with the Stanford Internet  
16      Observatory, I'm just not a hundred percent  
17      certain of the nature of it.

18              **Q.    Do you know whether he was involved**  
19      **in tracking misinformation and disinformation**  
20      **for the Stanford Internet Observatory?**

21              A.    I don't know if that intern was  
22      responsible for that or doing that work.

23              **Q.    Was that the only intern during**  
24      **2020 who was simultaneously working part time**  
25      **for CISA, and also working with Stanford**

1 **Internet Observatory?**

2 A. No. There was one other, as I  
3 mentioned earlier, there were two.

4 Q. And so, I see, in other words, it  
5 wasn't sequential. Those two interns, did they  
6 maintain their part-time internship at CISA  
7 through the election -- the end of the election  
8 cycle in 2020?

9 A. Correct. They were summer interns,  
10 full-time summer interns, and then they went  
11 back, they continued their studies at Stanford  
12 and part-time interns of us.

13 Q. Okay. So they also, I take it,  
14 when they went back to Stanford for the fall  
15 semester they also worked for the Stanford  
16 Internet Observatory?

17 A. That's my understanding, correct.

18 Q. And at least one of those interns  
19 was involved in doing these switchboarding  
20 e-mails like we're looking at in Exhibit 9;  
21 right?

22 A. Correct.

23 Q. Okay. What -- what did the other  
24 intern do during this timeframe for CISA?

25 A. He also did some of the

1 switchboarding.

2 Q. Okay. So should we add intern  
3 number two is also a -- a person who engages in  
4 switchboarding e-mails?

5 A. Correct.

6 Q. Are you declining to disclose the  
7 name of intern number two, as well?

8 A. Intern number two is on our staff  
9 now.

10 Q. What's his name?

11 A. Alex.

12 Q. Alex what?

13 A. Zaheer.

14 Q. So Alex Zaheer was -- was he one of  
15 the interns who originated the idea of the EIP?

16 A. Correct.

17 Q. What's his role in CISA now?

18 A. He is an analyst on the MDM team.

19 Q. What does he do for CISA?

20 A. He works on the MDM team. He  
21 does -- we talked about him earlier in the org  
22 chart discussion.

23 Q. I'm sorry, I don't remember, what  
24 does he do?

25 A. So he steps across the range of

1 work, he does some analysis, he does some  
2 engagement, he does some product development  
3 work.

4 Q. What's engagement? Does he talk to  
5 social media platforms for CISA?

6 A. He does not, no.

7 Q. Does he still do any work for  
8 Stanford Internet Observatory?

9 A. No, not that I'm aware of.

10 Q. When was he involved in working for  
11 Stanford Internet -- Stanford Internet  
12 Observatory, to your knowledge?

13 A. I don't know. It would have been  
14 before he graduated, as far as I'm aware.

15 Q. I'm asking you again, what's the  
16 name of intern number one, the one who was  
17 involved in routing disinformation concerns to  
18 social media platforms, during the 2020  
19 election, whose name you haven't disclosed yet?

20 A. I'm still not going to disclose his  
21 name.

22 MR. SAUER: Counsel, on the break  
23 let's talk about that.

24 BY MR. SAUER:

25 Q. Moving on a little bit, if I could

1 direct your attention back to -- or actually,  
2 let's jump ahead in the Exhibit 9. Actually,  
3 let me -- let's stay on this page.

4 A. Which page?

5 Q. I think we're on page 11 of the  
6 PDF.

7 A. Okay.

8 Q. Or actually, I'm sorry, let's jump  
9 ahead to page 10603 Bates, and then that's going  
10 to be page 18 of the PDF.

11 A. All right. Okay. I'm on page 18.

12 Q. Okay. If you look here, this is a  
13 reporting chain of a misinformation concern from  
14 you to Twitter, on October 10th; correct?

15 A. Yes, that's what it appears to be.

16 Q. And you're making this report at --  
17 on the Saturday afternoon; right? Or is that an  
18 early Saturday morning? It looks like it's a  
19 Saturday afternoon, at 12:52 p.m., there at the  
20 bottom of the page; do you see that?

21 A. I do.

22 Q. So you talked about this being  
23 resource intensive. Were you guys staffing, you  
24 know, the misinformation reports and doing the  
25 switchboarding on nights and weekends?

1           A.    So we ramped up as we got closer to  
2           the election.  At this stage I think it was  
3           primarily me that would receive them over the  
4           weekends.  I forget when we started -- when I  
5           started handing some of that off to my team to  
6           also pick it up over the weekends.

7                        But at some point, we did have  
8           people on the schedule.  It didn't mean that  
9           they were 24/7 waiting for things, they just  
10          needed to monitor their phones in case something  
11          came in.

12                    **Q.    How -- so somebody was kind of**  
13           **tasked with -- I think you called them shifts,**  
14           **earlier -- someone was tasked with covering a**  
15           **shift at all times, not at all times, but at**  
16           **times over the weekend?**

17                    A.    Yeah, particularly as we got closer  
18           to the election.  I wouldn't say it was the  
19           entire election cycle, it was -- I don't know  
20           when it started, but probably sometime in  
21           mid-October when -- when we started just shifts  
22           so that people could review, before that it was  
23           mostly me that would receive them from CIS.

24                    **Q.    And -- and then how about did you**  
25           **ever have it where you were doing shifts in the**



1 **meddling of the night.**

2 A. No. I mean, technically, you would  
3 be on for a day, if you're on your shift. But  
4 there wasn't an expectation, if something came  
5 in at 3:00 in the morning, that you were  
6 forwarding it on.

7 **Q. How because between 11:00 and 12:00**  
8 **at night?**

9 A. Yeah, I mean if you were awake at  
10 11:00 or 12:00 at night, I think that we would  
11 push it on, and then obviously on election --  
12 election night we were -- we were up until at  
13 least midnight. So if we received anything we  
14 would push it forward.

15 But again, it was more when we got  
16 into kind of off hours you just ask people to  
17 monitor their phones, if they could, and if  
18 something came in just to push it forward. But  
19 the expectation that, as per this e-mail, that  
20 they would be responsible for forwarding  
21 something.

22 **Q. Let me ask you this: If you look**  
23 **at this e-mail chain we're looking at, where it**  
24 **says you would forward on a concern at 12:52**  
25 **p.m., and looks like about 20 minutes later, on**

1 a Saturday afternoon, maybe Saturday morning,  
2 for them, Twitter responds and says: Thanks,  
3 Brian, we will escalate; do you see that?

4 A. Yes.

5 Q. So it looks like the people at  
6 Twitter are monitoring their phones to respond  
7 promptly to your reports; is that right?

8 A. I mean, that would -- I don't know  
9 what their monitoring behavior was, in this case  
10 she certainly responded relatively quickly on a  
11 Saturday.

12 Q. And that's not the only case, it  
13 happens again and again and again, where you get  
14 almost immediate responses from not just  
15 Twitter, but Facebook and others; correct?

16 A. I mean, don't know. I'd have to --  
17 I'm sure you could show me documents that would  
18 show that, but I honestly don't know the  
19 timelines of sends and returns.

20 Q. Well, you remember them pinging you  
21 back promptly and being very responsive when you  
22 would make reports like this?

23 A. They were generally responsive in  
24 making sure that we knew that they received it,  
25 yeah.

1 Q. And not just received it, for  
2 example, in this case, not long after that, at  
3 6:30 p.m. the same day, she notifies you: These  
4 tweets have actioned for violations of our  
5 policies; right?

6 A. That's what the e-mail says, yep.

7 Q. And was that timeframe typical,  
8 were they turning around, you know, content that  
9 was flagged and taking action on it within hours  
10 of your reports?

11 A. It's hard to say, because they  
12 didn't always get back to us if they hadn't  
13 taken any action. So I don't know if I would  
14 say that's typical.

15 You know, sometimes they would let  
16 us know, sometimes they wouldn't. Generally  
17 speaking, I think they made their decisions  
18 relatively quickly. So I would assume if they  
19 did get back to me it would be relatively  
20 quickly. But I can't speak to their timing or  
21 their processes or any of that stuff. A lot of  
22 times they just didn't let us know --

23 Q. But the more response --

24 A. -- to be honest, if they received  
25 it.

1 Q. Sorry to interrupt.

2 A. Yeah, I just wanted to say,  
3 normally we would get a note that they received  
4 the messages I forwarded to them. We often  
5 didn't receive any kind of notification that  
6 they had taken action, no action, or what their  
7 decision was, so it's hard to say kind of what  
8 their typical timeline was for making decisions.

9 Q. Let me ask you this: Were they  
10 more responsive to you, as a representative of a  
11 federal national security agency, than they were  
12 to ordinary people who made such reports, if you  
13 know?

14 MR. GARDNER: Objection.  
15 Objection, lack of foundation, calls for  
16 speculation.

17 A. Yeah, I have no clue. I don't know  
18 what the timeline was, generally.

19 Q. Were there ever discussions between  
20 you or anyone at CISA and any one of the  
21 platforms about making sure the platforms are  
22 monitoring their e-mails for the -- the  
23 government's reports of misinformation?

24 A. No.

25 Q. How about in the synch meetings

1 that you talked about, between the USG and the  
2 industry, was it ever brought up that, hey, you  
3 know, we're going to have people standing by and  
4 watching for misinformation reports so we can  
5 move quickly on them?

6 A. Not that I recall. I believe on  
7 election night several of the platforms set up  
8 their own operations center. But I don't know  
9 that there's ever a conversation about -- from  
10 the government expecting platforms to have any  
11 particular timeline.

12 Q. Again, these sort of e-mail --  
13 e-mails that we're looking at here in Exhibit 9,  
14 from you to the platform and the platforms  
15 responding back about misinformation that you  
16 guys have switchboarded to them, I take it  
17 there's a set of e-mails like this, for not just  
18 you, but also for Chad Josiah, Rob Schaul, Alex  
19 Zaheer, John Stafford, and an intern that you  
20 haven't named yet; right?

21 MR. GARDNER: Objection, compound.

22 A. So if I'm understanding your  
23 question, would you find e-mails from those  
24 individuals to platforms notifying them or  
25 forwarding information from an election

1 official, so yes.

2 Would there likely be -- it's hard  
3 for me to know if -- if they always responded  
4 back, beyond the received, which I think was  
5 pretty standard.

6 So I would assume that you would  
7 find change with other members of the team,  
8 where they sent something over to a platform and  
9 the platform said received, so yeah, if that's  
10 your question.

11 **Q. So in other words, at least those**  
12 **five individuals I just listed were involved,**  
13 **separate from the e-mails that we're looking at**  
14 **that involved you, they were sending their own**  
15 **e-mails, when it was their shift, to social**  
16 **media platforms, flagging disinformation**  
17 **concerns?**

18 A. Yeah, that's correct. But keep in  
19 mind, over the entire course of the election I  
20 think we forwarded about 200 e-mails, total. So  
21 I would imagine the vast majority of them are  
22 mine, because for a period of time I was the  
23 principal one relaying it.

24 But then to answer your question,  
25 yes, there's probably other e-mail chains with

1 those five representatives on it.

2 MR. GARDNER: So we've now been  
3 going almost two hours. I think now would  
4 probably be a good time for a break.

5 MR. SAUER: Let me ask one more  
6 question, that's right on this topic, and how  
7 about that or one little set of questions.

8 MR. GARDNER: Sure.

9 BY MR. SAUER:

10 Q. Did you ever discuss with Alex  
11 Zaheer what he did for the Election Integrity  
12 Partnership?

13 A. I'm sure I had conversations with  
14 Alex about his work with SIO, which was part of  
15 the larger integrity partnership.

16 Q. What did you discuss with him about  
17 his work for SIO?

18 A. I think he just talked about that  
19 he was participating in it, I don't know the  
20 specifics of the conversation, but that he was  
21 participating in it, and he was one of the  
22 people that were working with the ticketing  
23 system.

24 Q. When you say: Working with the  
25 ticketing system, what did he say he was doing

1       **with the ticketing system?**

2               A.    I don't recall.  I mean, I was -- I  
3       don't know how the ticketing system works, so I  
4       don't know, kind of, how his role would have  
5       played in there, what it was.

6               **Q.    When you refer to the ticketing**  
7       **system, is that the system that Stanford had for**  
8       **receiving reports of disinformation that they**  
9       **would analyze?**

10              A.    Correct.

11              **Q.    How about the other intern, the one**  
12       **you haven't named yet, did you ever discuss with**  
13       **that intern the work he did for the Stanford**  
14       **Internet Observatory?**

15              A.    I don't -- I don't recall.  I don't  
16       think -- certainly not in the level of detail  
17       with Alex.  Obviously Alex came to work for us,  
18       so I have a little more familiarity with what he  
19       did with SIO.  So I don't -- I didn't have a  
20       clear understanding of the other intern's role.

21              **Q.    What did the other intern go on to**  
22       **do?**

23              A.    I don't know.  As far as I know,  
24       he's still at Stanford.  But I don't know if he  
25       graduated.



1 MR. SAUER: Why don't we take a  
2 break there.

3 MR. GARDNER: Okay. I mean, it is  
4 now -- oh, let's go off the record.

5 THE VIDEOGRAPHER: The time is now  
6 12:34. We're off the record.

7 (Recess.)

8 THE VIDEOGRAPHER: The time is now  
9 1:41 p.m. We are back on the record.

10 MR. GARDNER: Thank you. And as I  
11 had mentioned before we got back on the record,  
12 the witness wanted to say something before we  
13 began.

14 THE WITNESS: So the intern that  
15 did both SIO and CISA push forwarding was Pierce  
16 Lowary.

17 BY MR. SAUER:

18 Q. And is that L-o-w-a-r-y?

19 A. I believe so, yeah.

20 Q. And that intern worked  
21 simultaneously with CISA and the EIP?

22 A. And SIO was a member of the EIP.

23 Q. Right. What did he do for SIO  
24 while this was going on, do you know?

25 A. I don't.

1 Q. What did he do for CISA while this  
2 was going on?

3 A. Again, he was part-time in the  
4 fall, so he would support the analytic stuff,  
5 and then, as I mentioned, he did some work in  
6 terms of the switchboarding. I'm not --  
7 obviously not sure the extent of the e-mails or  
8 anything like that, that he would have forwarded  
9 over to the platforms.

10 Q. Now, Pierce Lowary was involved in  
11 forwarding e-mails over to the platforms?

12 A. Correct.

13 Q. And that's in addition to Chad  
14 Josiah, Rob Schaul, Alex Zaheer, John Stafford,  
15 and yourself; correct?

16 A. Correct.

17 Q. Anyone else, in 2020, who would  
18 engage in those switchboarding e-mails?

19 A. I believe that was all.

20 Q. Was Pierce --

21 A. From my recollection.

22 Q. Was Pierce Lowary one of the four  
23 interns who originated the idea of the EIP?

24 A. Yes.

25 Q. Okay. Who were the other two?

1 A. I don't --

2 Q. Well, let me -- what about Alex  
3 Zaheer, was he one of the ones?

4 A. Alex was one.

5 Q. The idea --

6 A. It got --

7 MR. GARDNER: Hold on, guys, you  
8 keep talking over each other. So let Mr. Sauer  
9 ask the question and then please answer.

10 John, can you re-ask it?

11 BY MR. SAUER:

12 Q. Was Alex Zaheer one of the four  
13 interns who originated the idea of the EIP?

14 A. He was.

15 Q. And he went on, like Mr. Lowary, to  
16 simultaneously work for CISA and for Stanford  
17 Internet Observatory during the 2020 election  
18 cycle?

19 A. Correct.

20 Q. Who were the other two interns who  
21 originated the idea?

22 A. The fourth intern I do not know who  
23 they're referring to, so I'm not sure who that  
24 is.

25 The first intern is Isabella

1 Camargo, I forget the rest of her last name, I'm  
2 sorry. I'd have to look.

3 Q. Is it Isabella Garcia-Camargo?

4 A. Yes.

5 Q. Okay. When did she intern for  
6 CISA?

7 A. Over the summer of 2020.

8 Q. Did she do that into the fall?

9 A. She did not.

10 Q. Did she go on in the fall to work  
11 for Stanford -- Stanford Internet Observatory?

12 A. Yes.

13 Q. And did she work for Stanford  
14 Internet Observatory during the summer, when she  
15 was also working for CISA?

16 A. Yes.

17 Q. Who is Ayelet Drazen, D-r-a --

18 A. Hold on a second, I'm sorry, can  
19 you repeat that last question?

20 Q. Which question, who is Ayelet  
21 Drazen?

22 A. No, the one before.

23 Q. Did she work for Stanford Internet  
24 Observatory during the time she was also working  
25 for CISA?

1           A.    I don't believe so, but I'm not  
2           sure kind of their arrangement in the SIO front.  
3           I think SIO was -- I think SIO may have been --  
4           I'm not sure how that worked with SIO when  
5           they're interns, but she did not work for us in  
6           the fall, when she was working for SIO, that I'm  
7           certain of, so I don't know what the  
8           relationship was over the summer internship.

9           **Q.    What -- what did she do for CISA?**

10          A.    Again, like the other analysts,  
11          typical intern stuff, supporting product  
12          development, helping with, you know, any  
13          research projects, standard kind of intern work  
14          across the three panels I mentioned before,  
15          engagement, product development, and analysis  
16          research.

17          **Q.    Who is Ayelet Drazen, D-r-a-z-e-n,**  
18          **first name A-y-e-l-e-t?**

19          A.    I don't know.

20          **Q.    Who is Ashwin Ramaswami?**

21          A.    I believe he was one of the  
22          election security interns.

23          **Q.    During 2020 at CISA?**

24          A.    At least the summer of 2020. I  
25          don't -- I don't know, kind of, how long he

1 stuck around. I didn't really work with him.

2 **Q. Is he another Stanford intern?**

3 A. Yeah, I believe so.

4 **Q. Did he go on to work for the**  
5 **Stanford Internet Observatory?**

6 A. I don't know. I don't know.

7 **Q. How about Jack Cable, C-a-b-l-e?**

8 A. He was a Stanford intern. I  
9 don't -- I don't know what he did, after, just  
10 for the summer, that I'm aware of, but I'm not  
11 entirely sure. He didn't work on the MDM stuff  
12 with me.

13 **Q. What did he do at CISA, do you**  
14 **know?**

15 A. He was more cyber-focused, so I'm  
16 not entirely sure, really, what his projects  
17 are.

18 **Q. Just a second, I'm e-mailing you**  
19 **two new exhibits.**

20 **Let me ask this: Were you involved**  
21 **in -- Mr. Scully, were you involved in preparing**  
22 **CISA's discovery responses to written discovery**  
23 **in this case?**

24 A. I believe I provided names of the  
25 team. And the IT folks searched my records for

1 me.

2 Q. You provided names?

3 A. Don't ask --

4 Q. Names of the team, what does that  
5 mean?

6 A. So I believe I provided names of  
7 the people who are part of the MDM team or the  
8 CFITF.

9 Q. So you provided names of key  
10 custodians, for example, who might have relevant  
11 e-mails in their inboxes, stuff like that?

12 A. Right.

13 Q. Okay. Were you involved in  
14 drafting interrogatory responses?

15 A. If I recall correctly, I reviewed  
16 some of them.

17 Q. Did you review the ones that were  
18 submitted on behalf of CISA?

19 A. Yeah, those would have been the  
20 only ones I reviewed.

21 Q. Before the break, you mentioned  
22 that there were about 200 e-mails that CISA  
23 forwarded to serve this switchboarding function  
24 of routing disinformation concerns to the social  
25 media platforms in 2020; right?

1 A. Yeah, give or take a few. I don't  
2 know the exact number, but it's about 200.

3 Q. How do you know how many there  
4 were.

5 A. Well, as I mentioned previously, we  
6 kept a tracking spreadsheet. Everything we sent  
7 over we logged.

8 Q. Would you consult that tracking  
9 spreadsheet when you were preparing or working  
10 on responding to written discovery in this case?

11 A. I don't recall that I did, it's  
12 possible, but I don't recall doing it.

13 (Exhibit No. 12 was marked for  
14 identification.)

15 BY MR. SAUER:

16 Q. Let me show you Exhibit 12.

17 A. Okay. That's a complaint.

18 Q. It should be amended interrogatory  
19 responses that have also been filed publicly  
20 with the Court as document 86-3?

21 MR. GARDNER: I'd like to take a  
22 look. Hold on.

23 THE WITNESS: I don't know.

24 MR. GARDNER: Hold on one sec.

25 Yeah, that's right. That's right.



1 THE WITNESS: Okay.

2 BY MR. SAUER:

3 Q. Can you go to page 19 of that  
4 document? I've also got it up on the screen  
5 share.

6 A. All right. Page 19? Okay. I'm at  
7 19.

8 Q. In here, at the bottom of page 19,  
9 you see where it says: CISA, colon?

10 A. Yes.

11 Q. It's identifying people with  
12 relevant communications response to our  
13 discovery requests.

14 CISA has identified the following  
15 custodians as having relevant communications as  
16 produced in the response to requests two and  
17 three; correct? Do you see that?

18 A. I do.

19 Q. CISA custodians listed are Jen  
20 Easterly, Christopher Krebs, Matt Masterson,  
21 Geoff Hale, Brian Scully, and Lauren Protentis;  
22 right?

23 A. Yep.

24 Q. So these other people, Chad Josiah,  
25 Rob Schaul, Alex Zaheer, John Stafford, Pierce

1 Lowary, who were involved in forwarding e-mails  
2 to social media platforms to flag them, were not  
3 disclosed in this part of the interrogatories;  
4 correct?

5 A. I think if you scroll down another  
6 paragraph, you would see most of those names.

7 Q. Yeah, that's extremely interesting,  
8 isn't it? Very next paragraph it says, oh,  
9 we've also identified some other people as  
10 appearing in the communications you produced,  
11 and it lists four of those five people, Chad  
12 Josiah, Robert Schaul, Alex Zaheer, John  
13 Stafford; right?

14 A. Yes, that's who is listed there.

15 Q. It appears --

16 A. I don't know that that's  
17 interesting.

18 Q. It's interesting that CISA knew  
19 about the involvement of these people and  
20 relevant communications, but didn't search their  
21 inboxes in response to our discovery requests;  
22 isn't that what this indicates?

23 A. I have no idea what this indicates.

24 Q. Well, let me ask you this: You  
25 testified before the break that those four

1 people there, plus Pierce Lowary, who you just  
2 disclosed, all forwarded disinformation reports  
3 to social media platforms as part of the  
4 switchboarding function; isn't that right?

5 A. They were all part of the  
6 switchboarding function. I don't know who sent  
7 e-mails or how many e-mails or any of that.

8 Q. But you testified that they took  
9 shifts and sent e-mails to social media  
10 platforms reporting this information; correct?

11 A. They took shifts, and if they  
12 received something they would have sent an  
13 e-mail. But without going through the  
14 spreadsheet that I mentioned I wouldn't know if  
15 an actual individual was on a shift, sent one,  
16 but that would be my expectation that they did.

17 Q. What was the last --

18 A. There were generally two people  
19 per -- there were generally two people per  
20 shift, so it's possible that just one of those  
21 two people were sending e-mails.

22 Q. Pierce Lowary is not identified  
23 anywhere in these discovery responses, is he?

24 A. I mean, he's not identified in  
25 these. This is a small section. I don't know

1 if he is elsewhere.

2 Q. Well, you said you reviewed them  
3 when they were being prepared. Do you remember  
4 seeing his name anywhere -- anywhere in the  
5 government's discovery responses?

6 A. I don't recall, but I wouldn't  
7 have -- I don't think I would have reviewed the  
8 entire document, so I don't know.

9 Q. Who would have --

10 A. Obviously, I didn't see the final  
11 document.

12 Q. Who would have reviewed the final  
13 document?

14 MR. GARDNER: Objection, calls for  
15 speculation.

16 BY MR. SAUER:

17 Q. If you know.

18 A. Yeah, I don't know.

19 MR. SAUER: Exhibit 62, which I've  
20 also e-mailed you.

21 MR. GARDNER: John, did you say 62?

22 MR. SAUER: 62, should be the most  
23 recent one in your inbox.

24 THE WITNESS: Okay. Okay.

25 (Exhibit No. 62 was marked for

1 identification.)

2 BY MR. SAUER:

3 Q. Here's Jack --

4 A. Is it the -- sorry, go ahead.

5 Q. This is Jack Cable's publicly  
6 available online LinkedIn profile; do you see  
7 that?

8 A. I do.

9 Q. If you scroll down, a fifth page of  
10 this document, it looks like he was a research  
11 assistant at Stanford Internet Observatory from  
12 2019 to 2021; correct?

13 A. That's what it says, yep.

14 Q. And that he ended in June of 2021,  
15 correct, at SIO?

16 A. That's what it says, yeah.

17 Q. And immediately below that, it  
18 looks like he was an election security technical  
19 advisor at CISA from June 2020 to January 2021;  
20 correct?

21 A. That's what he says.

22 Q. So he also overlapped, for an  
23 entire year, in working simultaneously for CISA  
24 and for the SIO; correct?

25 MR. GARDNER: Objection, lack of

1 foundation.

2 BY MR. SAUER:

3 Q. According to his LinkedIn profile?

4 MR. GARDNER: Same objection.

5 A. LinkedIn profile says he worked at  
6 CISA for eight months.

7 (Reporter admonition.)

8 THE WITNESS: Sorry.

9 A. The LinkedIn profile said he worked  
10 at CISA for eight months.

11 Q. Right. Does the LinkedIn profile  
12 also indicate that during those same eight  
13 months, from June of 2020 to January of 2021, he  
14 also was an intern -- a research assistant at  
15 Stanford?

16 A. It appears that way, yep.

17 Q. Were you aware that Jack Cable was  
18 working for Stanford Internet Observatory while  
19 he was also interning for CISA?

20 A. No. Jack didn't work for me, so I  
21 didn't really pay attention to what he was  
22 doing.

23 Q. He shares this simultaneous  
24 employment with SIO and CISA, along with Alex  
25 Zaheer and Pierce Lowary; correct?

1 MR. GARDNER: Objection, lack of  
2 foundation.

3 BY MR. SAUER:

4 Q. Correct?

5 A. I'm sorry, could you repeat the  
6 question?

7 Q. Pierce Lowary and Alex Zaheer also  
8 simultaneously worked for CISA and SIO; correct?

9 A. They did.

10 Q. And then, if you scroll up a little  
11 bit, to the page before, it looks like he went  
12 on to work for the Krebs-Stamos Group; were you  
13 aware of that?

14 A. No, I don't think so.

15 Q. And then he went on to work for the  
16 senate; correct? Does that ring a bell?

17 A. I mean, it's what it says here.

18 Q. So you didn't know what Jack Cable  
19 went on to do after he left CISA?

20 A. No, I didn't really pay attention  
21 to what -- like I said, he didn't work for me,  
22 so I didn't really follow him. In fact, I'm --  
23 a couple of my interns I'm not sure what they're  
24 doing, either.

25 Q. Let's go back to Exhibit 9.

1                   Is it possible that Jack Cable was  
2                   another one of the interns who originated the  
3                   EIP? You mentioned there's one, and you're not  
4                   sure if it was them?

5                   MR. GARDNER: Objection, calls for  
6                   speculation.

7                   A. Yeah, I wouldn't know. I wouldn't  
8                   know.

9                   Q. Let's go to page 8769 in this  
10                  document, Exhibit 9.

11                  A. Do you know what the PDF page is,  
12                  John?

13                  Q. I'm scrolling down to it, so I'll  
14                  tell you as soon as I know the answer.

15                  A. Okay.

16                  Q. I think it's PDF page 62.

17                  A. All right.

18                  Q. All right. If you see here, it  
19                  looks like Alex Zaheer, on October 30th, sends a  
20                  report about misinformation to CFITF, which is  
21                  the CISA reporting e-mail address; correct?

22                  MR. GARDNER: John, I'm sorry, are  
23                  you going to post this on the -- on the live  
24                  screen for us?

25                  MR. SAUER: I'm sorry, I didn't



1 realize it wasn't up. Can you see it on the  
2 screen share?

3 MR. GARDNER: Yeah, we got it now.

4 Thank you.

5 BY MR. SAUER:

6 Q. Alex Zaheer, on October 30th, sends  
7 an e-mail to CFITF; correct?

8 A. Yep.

9 Q. And he's actually --

10 A. Yes.

11 Q. He says: FYSA, EIP has reported  
12 the following to EI-ISAC and Twitter from EIP,  
13 and then he reports on an EIP ticket; correct?

14 A. Correct.

15 Q. And then this -- you responded to  
16 him, Thanks Alex; do you see that on the page  
17 before?

18 A. Yes.

19 Q. And then you sent an e-mail, it's  
20 not clear to whom, saying: FYI, the EIP,  
21 submitted the below to Twitter, no need to  
22 respond. But it looks like you were saying that  
23 to Twitter; right?

24 A. Yeah, there's no header there, so  
25 I'm not certain, but that's what it appears.

1 Q. It appears that from your intern,  
2 who was simultaneously working for EIP, you  
3 received a report of alleged misinformation and  
4 submitted it onto Twitter; right?

5 A. Yeah.

6 Q. And then -- and that was an  
7 EIP-specific report; correct?

8 A. Yep.

9 Q. And then Twitter responded and  
10 said, thanks Brian, we received that report from  
11 the EIP and escalated it; correct?

12 A. Yes.

13 Q. And then she goes on to specify to  
14 you the action they took against that; correct?

15 A. Yeah, on a contextual label  
16 pursuant to their policy on civic integrity,  
17 yeah.

18 Q. Were there other instances where  
19 this occurred, where an EIP report was forwarded  
20 to you, and you forwarded it onto -- to a social  
21 media platform?

22 A. As I said earlier, it's possible,  
23 but I don't recall.

24 Q. How about --

25 A. It was our standard practice.

1 Q. How about the other five people who  
2 were monitoring these misinformation reporting  
3 e-mails, did they ever review that, do you know?

4 MR. GARDNER: Objection, calls for  
5 speculation.

6 A. Yeah, I don't know. Again, it  
7 wasn't part of our normal process, so I'm not  
8 sure.

9 Q. Would that be reflected in this  
10 spreadsheet you referred to multiple times?

11 A. Yeah, it should be.

12 Q. So if there was -- if the EIP is  
13 referenced or is the originator of the report  
14 you would note that in the spreadsheet?

15 A. I believe so. I believe we would  
16 have the case number.

17 Q. Can you scroll back up to page 33  
18 of the PDF?

19 A. Yep.

20 Q. It's Bates 8349.

21 A. 8349, yep.

22 Q. You see at the top of this page  
23 there's a misinformation report from Oregon,  
24 that's being sent on by the CIS, Center For  
25 Internet Security, reporting e-mail; do you see

1 that?

2 A. Yes.

3 Q. And it's sent to you and a couple  
4 other CISA e-mails or -- CISA e-mails, there in  
5 the first line; right?

6 A. Yep.

7 Q. In the second line it's sent to  
8 tips@2020partnership.atlassian.net; do you see  
9 that?

10 A. I do.

11 Q. What is that?

12 A. I don't know.

13 Q. Is that the reporting e-mail for  
14 tips to the 2020 Election Integrity Partnership?

15 MR. GARDNER: Objection, calls for  
16 speculation, also, asked and answered.

17 A. Yeah, I don't know what it is.

18 Q. Is it your testimony that you're  
19 not aware whether or not that's the reporting  
20 e-mail for the EIP?

21 A. Yeah, I'm not aware -- the answer  
22 is, I'm not aware of what e-mail that is.

23 Q. Were you aware that -- did you  
24 notice that CIS was commonly forwarding these  
25 reports to both you and that

1 **tips@2020partnership e-mail?**

2 A. I'm not sure that I paid that much  
3 attention to it, no.

4 **Q. You didn't notice --**

5 A. Again, yeah, I wasn't -- I guess  
6 that I wasn't aware of what processes they were  
7 following.

8 **Q. So you didn't know they were**  
9 **looping in the EIP on their reports; is that**  
10 **what you're saying?**

11 A. I don't recall it, but again, as we  
12 discussed earlier, it could have been part of  
13 the effort to deconflate for the platforms.

14 **Q. Up here on page 51 of the PDF,**  
15 **scrolling to the bottom of that page down to 52,**  
16 **here's another CIS report. Once again, it's**  
17 **sent to you at -- to CISA e-mails and**  
18 **tips@2020partnership@atlassian.net; correct?**

19 A. Yeah, I see the e-mail address in  
20 there.

21 **Q. And you don't recall that being --**  
22 **you getting copied -- that being copied on**  
23 **e-mails of this nature?**

24 A. I don't.

25 **Q. Really briefly, jumping ahead to**

1 page 10539, page 55, once again, CIS is copying  
2 you and tips@2020partnership.atlassian.net;  
3 correct?

4 A. That's the e-mail, yes.

5 Q. Jumping ahead to page 7565, here's  
6 a report from the Colorado secretary of state's  
7 office. Do you see, we're on page 59 of the  
8 PDF, where they're reporting it to EI-ISAC,  
9 CISA, and Stanford Partners; correct?

10 A. That's what the e-mail says, yep.

11 Q. It says Stanford is presumably --  
12 MR. GARDNER: Objection, calls for  
13 speculation.

14 A. Yeah, I don't know what they mean  
15 by Stanford.

16 Q. Do you think Stanford might be some  
17 other Stanford entity to which state and local  
18 election officials are reporting disinformation  
19 concerns --

20 MR. GARDNER: Objection.

21 BY MR. SAUER:

22 Q. -- during the 2020 cycle?

23 MR. GARDNER: Objection, calls for  
24 speculation, lacks foundation.

25 ///

1 BY MR. SAUER:

2 Q. Do you know?

3 A. I don't know.

4 Q. Scrolling above this, again, CIS  
5 forwards this to you and tips22020partnership,  
6 that reporting e-mail or that e-mail address;  
7 correct?

8 A. Are you up on -- what page are you  
9 on now?

10 Q. Page 58 of the PDF, immediately  
11 above, shows CIS forwarding that report from  
12 Colorado secretary of state's office to both you  
13 and tips@2020partnership.atlassian.net?

14 A. So Colorado sends to CIS, CIS sends  
15 to me, CISA, and atlassian.net, okay.

16 Q. And you forward this onto -- to  
17 Twitter; correct, immediately above that?

18 A. So again, there's no header, but  
19 the response is from Twitter, so that's what I  
20 assume.

21 Q. And you -- they say -- you say:  
22 Please see below reporting from Colorado. These  
23 do not appear to be connected to the imposter  
24 parody accounts previously shared; correct?

25 A. Correct.

1 Q. And Twitter responds within 15  
2 minutes: We will escalate. Thank you; correct?

3 A. Correct.

4 Q. Okay. And if you scroll down a  
5 couple pages, you see that Colorado secretary of  
6 state's office has flagged some parody or  
7 imposter accounts, including one with 14  
8 followers; correct?

9 A. What page are you on?

10 Q. 59 of the PDF.

11 A. 59 of the PDF? I don't see what  
12 you're talking about there. This is the same  
13 e-mail chain we were just talking about.

14 Q. Maybe look up at the screen share,  
15 can you see where secretary of state's office  
16 has forwarded a screen shot of a Twitter  
17 account, it's got 14 followers?

18 A. I do.

19 Q. And secretary of state's office in  
20 Colorado says: These are concerning to us here  
21 in Colorado because of their recent FBI/CISA  
22 warnings about impersonation accounts; correct?

23 A. That's what it says, yep.

24 Q. So they say that we're reporting  
25 this because it -- because it's the sort of



1 things that the FBI and CISA warned us may  
2 warrant reporting; right?

3 A. I mean, I don't want to speak for  
4 the secretary of state, but that's kind of how  
5 the account sentence reads.

6 Q. Did you -- in fact, were you  
7 involved in warning state and local election  
8 officials about impersonation accounts spreading  
9 false information about the election?

10 A. I'm sure I would have reviewed a  
11 document that went out along those lines. I'm  
12 not aware of the document, but I'm sure if it  
13 went out I would have reviewed it.

14 Q. Do you remember reviewing it?

15 A. They put out -- in 2020 we put out  
16 a couple of joint FBI and CISA products. I  
17 don't remember specifically which one this is,  
18 but it certainly sounds like something we would  
19 do.

20 Q. Okay. Scrolling down, there's  
21 another one they're flagging here, that if you  
22 didn't know, it has two followers; correct?

23 A. So it appears.

24 Q. And you forwarded that onto  
25 Twitter, and Twitter said: We'll escalate;

1 right?

2 A. Yes. They said they will escalate.

3 Q. Moving onto page 10512, just a few  
4 pages down, that's going to be page 63 of the  
5 PDF.

6 A. Okay.

7 Q. Do you see here in the middle,  
8 here, it's an inquiry from Twitter, and she  
9 says: Hey Brian, can we talk about CIS  
10 misinformation reporting duplicate reports to  
11 EIP, possible to have just you escalate;  
12 correct?

13 A. Yeah, that's what the e-mail says.

14 Q. What is she talking about, is this  
15 the duplicate reporting issue that you talked  
16 about earlier, where they were getting reports  
17 from you and EIP and CIS?

18 A. That's what I would imagine it is,  
19 yeah.

20 Q. Okay. Do you remember anything  
21 about this? We're talking about October 27th,  
22 so, you know, maybe a week before the 2020  
23 election, do you remember the social media  
24 platform is having this concern about duplicate  
25 reports from CIS and EIP?

1           A.    I remember Twitter, in particular,  
2           having that concern.

3                    Our screen is screwy again.

4                    THE REPORTER:   Can we go off the  
5           record?

6                    MR. SAUER:   Yeah, we can go off the  
7           record.

8                    THE VIDEOGRAPHER:   The time is now  
9           2:11 p.m.   We're off the record.

10                   (Recess.)

11                   THE VIDEOGRAPHER:   The time is now  
12           2:13 p.m.   We are back on the record.

13   BY MR. SAUER:

14                   **Q.    Okay.  So -- and then, Mr. Scully,**  
15           **you responded to this:  So here's the deal, EIP**  
16           **will only report something to Twitter if they**  
17           **have additional context to provided based on**  
18           **their research; correct?**

19                   A.    That's what I wrote, yes.

20                   **Q.    How did you know that was going to**  
21           **be their policy or their practice, did you talk**  
22           **to EIP?**

23                   A.    I would imagine I did.

24                   **Q.    Who did you talk to?**

25                   A.    I don't recall.

1 Q. And that he goes on -- or you go on  
2 to say, they will not send Twitter reporting  
3 unless it has that additional context that would  
4 help you make a decision; correct?

5 A. Yep.

6 Q. And then it says: EIP will also  
7 let CISA know when they are reporting something  
8 to you so I can give you a heads up; correct?

9 A. Yep.

10 Q. Is that what happened after this  
11 e-mail, did EIP report to you when they were  
12 reporting something to the social media  
13 platforms?

14 A. I don't recall that, in practice.  
15 Although, obviously, we just went through each  
16 one e-mail that did that. I don't remember it  
17 being a common thing but, again, I don't -- I  
18 don't know. It's possible.

19 Q. Okay. And then it says: EIP will  
20 continue to use the CIA -- CIS case number to  
21 facilitate identifying duplicative reports;  
22 correct?

23 A. Yep.

24 Q. So EIP was talking to CIS enough to  
25 know what CIS's misinformation reporting case

1       **numbers were; right?**

2               A.    I don't know. I don't know if  
3       that's true.

4               **Q.    Were you aware that EIP was using**  
5       **CIS's case numbers, because you said it in this**  
6       **e-mail?**

7               A.    Yep, I mean, if that's what I  
8       wrote, that's probably what they were doing.

9               **Q.    Okay. Do you remember discussing**  
10       **that with CIS or EIP that they were going to,**  
11       **you know, kind of share case numbers?**

12              A.    I don't recall any such  
13       specificity. I know we had a conversation. I  
14       recall that we had conversations about how to  
15       de-duplicate, make sure we weren't overtaxing  
16       Twitter, in particular.

17              **Q.    And that de-duplication process**  
18       **involved some kind of coordination between you,**  
19       **EIP and CIS; correct?**

20              A.    Again, reading this, it appears we  
21       are just making sure we are sending something  
22       over and everybody is aware of it.

23              **Q.    Right. So everybody would tell**  
24       **everybody else that they were sending something**  
25       **over, and there was an attempt to avoid sending**

1           **duplicative reports to Twitter?**

2                           MR. GARDNER: Objection, compound.

3 BY MR. SAUER:

4                           **Q. Correct?**

5                           A. Yeah, can you -- can you break  
6 that -- can you start that over again?

7                           **Q. Was there an agreement for EIP and**  
8 **CIS and CISA to coordinate and let each other**  
9 **know what they were reporting to platforms like**  
10 **Twitter?**

11                          A. I think that's generally right,  
12 yeah.

13                          MR. SAUER: Let me send you a  
14 couple more exhibits, 10 and 11. I'm going to  
15 pull up 10 on the screen share while you're  
16 waiting.

17                          MR. GARDNER: John, do you -- John,  
18 did you send them over?

19                          MR. SAUER: Yeah. They should be  
20 in your inbox.

21                          MR. GARDNER: Yeah, I'm looking.

22                          MR. SAUER: They're in my sent box.

23                          MR. GARDNER: Okay. I believe you.

24 Hold on.

25                          (Exhibit No. 10 was marked for

1 identification.)

2 BY MR. SAUER:

3 Q. Let me ask this: Can you see it on  
4 the screen share?

5 A. I can.

6 MR. GARDNER: You haven't shared it  
7 yet, John.

8 THE WITNESS: Trick question.

9 BY MR. SAUER:

10 Q. Now can you see it on the screen  
11 share?

12 A. Yes.

13 Q. Just looking here at the first  
14 page, you know, this exhibit is a collection of  
15 your switchboarding e-mails from November of  
16 2020, do you see you, are copied here on  
17 misinformation report from CIS on November 2nd  
18 of 2020?

19 A. Yes.

20 Q. Once again, CIS continues to copy  
21 tips@2020partnership.atlassian.net; do you see  
22 that?

23 A. I do.

24 Q. Does that ring a bell for you about  
25 what that e-mail is, after we talked about that

1 last e-mail, where you were arranging to  
2 coordinate with EIP about de-duplicating reports  
3 to social media platforms?

4 A. I forget. I don't recall the  
5 e-mail. If you tell me that that was the tips  
6 for the 2020 EIP I would believe you.

7 Q. Okay. Let me scroll down a page to  
8 Bates 13603.

9 A. What page was that? I'm sorry.

10 Q. Bates 13603, 10 of the PDF.

11 A. Okay.

12 Q. You see here there's a report from  
13 the Iowa secretary of state's office on November  
14 2nd, that's sent to CIS; do you see that?

15 A. Just scrolling through it, sorry.  
16 Give me a second. Yes.

17 Q. And then it looks like the Iowa  
18 secretary of state's office also sent this to  
19 three FBI e-mail addresses; right, with the  
20 recipients redacted, FBI number two, FBI number  
21 three, and FBI number four; correct?

22 MR. GARDNER: Lack of -- objection,  
23 lack of foundation.

24 A. I don't see the e-mail addresses  
25 you're referring to.



1 Q. Do you see @FBI, if you look on the  
2 screen share, @FBI.gov?

3 MR. GARDNER: Same objections.

4 BY MR. SAUER:

5 Q. With the handle omitted, three  
6 e-mails?

7 A. Okay.

8 Q. Were you aware of the FBI being  
9 involved in receiving misinformation reports  
10 from state and local elections officials?

11 A. Generally speaking, we tell  
12 election officials to report what they saw to  
13 either DHS or the FBI, and it would end up where  
14 it needed to be.

15 Q. So you told them to report it to  
16 either DHS or the FBI?

17 A. Correct.

18 Q. Who at the FBI was receiving those  
19 kinds of reports?

20 A. I don't know. I think it --

21 Q. Go ahead.

22 A. Generally speaking, the FBI has  
23 field offices, and so the idea was if they  
24 were -- election officials had established  
25 relationships with the FBI field office and the

1 elections coordinator in that office, and that's  
2 where they wanted to report it, that they could  
3 do so.

4 **Q. So there was -- these FBI officials**  
5 **tended to be FBI field officers -- officers?**

6 A. I don't want to speculate, but --  
7 but again, that was, you know, us trying to --  
8 to help the election officials, just if they had  
9 something they needed to report, if they had as  
10 many different options to do that as possible.

11 **Q. Okay. Do you know what FBI did**  
12 **with its misinformation reports, was it**  
13 **switchboarding them like you guys were doing?**

14 A. I don't know, to be honest.

15 **Q. Is that notion that you could**  
16 **forward things to the FBI, is that something**  
17 **that was discussed in those USG**  
18 **industry-specific meetings you talked about?**

19 A. I -- not that I recall, but it's  
20 possible we -- we talked to them about the  
21 guidance we gave to election officials, that  
22 election officials could it either way, but I  
23 don't recall specific conversations along those  
24 lines.

25 **Q. Can you scroll down to the page 27**

1 of the PDF.

2 A. Let's go. Okay.

3 Q. If you look here, kind of at the  
4 bottom of this text chain, Aaron Wilson, he's  
5 your contact at CIS; right?

6 A. Correct.

7 Q. And he's forwarding something to --  
8 November 3rd, with a report about alleged  
9 election misinformation; right?

10 A. Well, poll worker Erie PA says  
11 announces on Instagram they will throw away  
12 Pro-Trump votes, that's what you're talking  
13 about?

14 Q. Yeah.

15 A. That's the subject of the e-mail.

16 Q. He uses the EIP case number for  
17 this report; correct?

18 A. He does.

19 Q. And he sent it to CISA at the CFITF  
20 e-mail; correct?

21 A. He does, correct.

22 Q. And the CFITF e-mail forwards it to  
23 you, and you forward it to Matt Masterson at  
24 Facebook; correct?

25 A. No, that's not correct. I -- Matt

1 was still at CISA at the time. I forwarded it  
2 to Saleela Salahuddin at Facebook.

3 **Q. Copying Matt Masterson?**

4 A. I'm sorry?

5 **Q. Copying Matt Masterson?**

6 A. Yeah, who was at CISA. You said he  
7 was at Facebook. I just wanted to make sure  
8 that that was clear that he was still --

9 **Q. I'm sorry, I meant to say and**  
10 **Facebook, not at Facebook?**

11 A. Gotcha.

12 **Q. And then Facebook came back to you**  
13 **for clarification; right? Do you recall that?**

14 A. So we -- sorry, go ahead.

15 **Q. Go ahead, what were you going to**  
16 **say?**

17 A. I said, just to be clear, we  
18 forwarded the statement from Pennsylvania about  
19 that incident to Facebook and Matt Masterson.

20 **Q. And so --**

21 A. That's what is here.

22 **Q. And they -- and it looks like**  
23 **Facebook asked you, could you please confirm**  
24 **that, A, the worker in question who was**  
25 **supposedly destroying Pro-Trump ballots is not a**

1 poll worker, or B, that he did not, in fact,  
2 destroy ballots or at least there's no evidence  
3 he did.

4 So Facebook asked you, Brian Scully  
5 and Matt Masterson, for that clarification;  
6 right?

7 A. They did.

8 Q. Yeah, and then you responded: Not  
9 sure I understand the distinction you're trying  
10 to make, but both components of the narrative  
11 are false. The person is not a poll worker and  
12 no ballots were destroyed. I suppose that makes  
13 the entire thing a hoax; correct?

14 A. Yeah, that was my response.

15 Q. What was your basis for concluding  
16 that both components of the narrative were  
17 false?

18 A. I believe the statements from  
19 Pennsylvania. I assume if you have that  
20 document we can take a look and confirm.

21 Q. You read the statement from  
22 Pennsylvania and reported its content back to  
23 Facebook?

24 A. Correct.

25 Q. Okay. Did you -- did that happen

1 from time to time, where you wouldn't just  
2 forward the disinformation concern, but then you  
3 would provide, you know, information that would  
4 help debunk it through the social media network?

5 A. I think I frame it a little  
6 differently, if social media platforms needed  
7 additional information from an election official  
8 we would try to support that. There was also  
9 one time when I believe it was Facebook had a  
10 question about DHS immigration and customs  
11 enforcement having agents going places where we  
12 also provided a response back on a specific  
13 piece.

14 But generally speaking, we would do  
15 what we did here, which is if the -- if the  
16 jurisdiction made a public statement or if there  
17 was additional information the jurisdiction  
18 could provide, and the platforms asked for it,  
19 that we would try to facilitate getting the  
20 information they asked for.

21 Q. Did you merely relay that  
22 information, the sort of debunking information  
23 from the election official, would you sometimes  
24 find it on your own and helpfully supply it to  
25 the social media platform?

1           A.    If it was a public statement, I'm  
2           sure we pulled it ourselves.  If there was not a  
3           public statement, I would imagine we would go  
4           back to the election official.

5           **Q.    But you might --**

6           A.    I don't know --

7           **Q.    Go ahead.**

8           A.    Sorry, I don't want to say that  
9           every case was exactly like that, but again, if  
10          there was a public statement that was put out by  
11          the jurisdiction, we would -- we would defer to  
12          that.

13          **Q.    Did you take any steps to find**  
14          **out -- for example, suppose there's a public**  
15          **statement that disputes what a private citizen**  
16          **has said on Facebook or Twitter, would you do**  
17          **further research to figure out who was telling**  
18          **the truth or would you just relay the official**  
19          **government explanation of the incident to the**  
20          **social media platforms?**

21          A.    We would relay the -- the official  
22          statement from the jurisdiction.

23          **Q.    I take it sometimes you would go**  
24          **find that official statement on your own, and**  
25          **sometimes you would reach out to the state or**

1       **local jurisdiction to see if they issued a**  
2       **statement?**

3               A.     Yeah, we would find, I think it  
4       implies that we were doing a rigorous search.  
5       Generally, we would be aware if a jurisdiction  
6       put out a statement and we would just pull it  
7       ourselves.

8               **Q.     Look ahead to --**

9               A.     And sometimes --

10              **Q.     Go ahead.**

11              A.     Sorry.

12                         Sometimes we would reach out to the  
13       jurisdiction and they would just provide the  
14       statements that they had already made public, as  
15       well.

16              **Q.     Would you relay that to the social**  
17       **media platform?**

18              A.     Yeah, if they were asking for  
19       additional information we would.

20              **Q.     Here's another one, page 35 of the**  
21       **PDF, Bates 8663. Do you see that on the screen**  
22       **share?**

23              A.     I'm scrolling down to it. 8663?

24              **Q.     Yeah.**

25              A.     Yep.



1 Q. And here in this e-mail chain it  
2 looks like it's another situation where Twitter  
3 asked for some clarification, for example, she  
4 says, on November 6th, have Pennsylvania state  
5 officials provided initial information to you on  
6 the authenticity of the video or the  
7 circumstances under -- underpinning it; do you  
8 see that?

9 A. I do.

10 Q. And then you respond, scrolling  
11 back up, you say: There are two reports in the  
12 e-mail chain, and you explain what you  
13 understand what Pennsylvania is saying about the  
14 disputed information; right?

15 A. Sorry, I'm just scrolling down to  
16 make sure I understand the context of the chain.

17 Okay. Sorry. Could you repeat the  
18 question?

19 Q. Sure. My question is: You  
20 provided clarification to the social media  
21 platform about what you believe the Pennsylvania  
22 reporter meant; correct?

23 A. I don't believe that is correct.

24 Q. Well, did you say, for example, on  
25 the authenticity Pennsylvania states in the very

1 first e-mail that they believe the videos are  
2 false and we're reaching out to our partners to  
3 validate; correct?

4 A. Correct.

5 Q. Okay. And then, later that day, if  
6 you scroll up, you say: Hey, to Twitter, just  
7 came across this debunk of the video on Twitter;  
8 correct?

9 A. Yes.

10 Q. And then -- so you are looking  
11 around to find information that would debunk it;  
12 correct?

13 A. I don't know if that's correct.  
14 It's possible somebody just let us know that  
15 there was something there.

16 Q. And then 17 minutes later Twitter  
17 responds, thank you so much, we applied a label  
18 to the tweet; correct?

19 A. Yes, that's what they said back,  
20 correct.

21 Q. Scroll down to page 8669.

22 A. What page of the PDF?

23 Q. 46.

24 A. 46?

25 Q. Yes. And here you've got a

1           misinformation report from the secretary of  
2           state of Arizona's office; do you see that?

3           A.     Yes.

4           Q.     It says: This post is on a private  
5           Facebook page, above. I've included a screen  
6           shot; correct?

7           A.     That's what the Arizona e-mail  
8           says, yep.

9           Q.     How did they -- was that unusual  
10          for them to report statements on a private  
11          Facebook page?

12          A.     I don't -- I don't know. We didn't  
13          do any analysis of that kind.

14          Q.     Okay. So you don't know whether  
15          someone was monitoring how posts appeared on a  
16          private Facebook page containing alleged  
17          misinformation?

18          A.     I don't know how Arizona secretary  
19          of state came across that information, no.

20          Q.     Dropping ahead to page 864, now.  
21          Here at 954 --

22          A.     I'm sorry.

23          Q.     Sorry.

24          A.     54?

25          Q.     Oh, sorry, page 54 of the PDF, yes,

1       **sorry. Actually, no, I'm sorry, that's not the**  
2       **right page.**

3           A.    Okay.

4           Q.    **No, sorry, page 59 of the PDF?**

5           A.    59? Okay.

6           Q.    **Here's a chain on Tuesday, November**  
7       **10th, at 7:23 in the evening, you forwarded a**  
8       **report of information -- misinformation to**  
9       **Twitter; correct, at 7:23?**

10          A.    Yeah, that's what appears, there's  
11       no he header on the e-mail, but considering the  
12       responses is from Twitter, I assume that's who I  
13       sent it to.

14          Q.    **And Twitter responds in two**  
15       **minutes, we will escalate; right?**

16          A.    Yep.

17          Q.    **And then Twitter responds here a**  
18       **few minutes later, after midnight, at 12:11**  
19       **a.m., hey, we labeled all the tweets except two;**  
20       **right?**

21          A.    Yes.

22          Q.    **So Twitter was working on this well**  
23       **into the evening, along with -- were you guys**  
24       **doing that well into the evening?**

25                   MR. GARDNER: Objection, compound.

1 BY MR. SAUER:

2 Q. Timeframe?

3 A. So was Twitter working on it well  
4 into the evening? I mean, I guess. Were we?  
5 Again, if somebody was checking the phone, most  
6 of the post-election stuff would have been me.  
7 We would have done something with it, but it  
8 wasn't a requirement.

9 (Exhibit No. 11 was marked for  
10 identification.)

11 BY MR. SAUER:

12 Q. And showing you Exhibit 11, which  
13 should be in your inbox.

14 MR. GARDNER: Yeah, I think that's  
15 right.

16 A. Okay.

17 Q. On the last page of this PDF,  
18 there's an e-mail from Aaron Wilson?

19 MR. GARDNER: I'm sorry, John, do  
20 you want to post it on the screen?

21 MR. SAUER: Oh, thank you.

22 MR. GARDNER: You don't need to, if  
23 you don't want to, I mean, we have the --

24 MR. SAUER: I got it, I mean, I  
25 thought it was up.

1 BY MR. SAUER:

2 Q. Last -- see it, last page of the  
3 PDF, there's a report from CIS.

4 A. Yeah.

5 Q. Actually, this is, interestingly, a  
6 report from CIS to Gwinnet County; right? Where  
7 they say: Hi Kristi, the EI-ISAC and our  
8 partners at the Election Integrity Partnership  
9 are tracking a social media post that's getting  
10 traction very quickly; right?

11 A. Yes, that's what the e-mail reads,  
12 yeah.

13 Q. So this is a situation where the  
14 reporting was actually originated by CIS or EIP  
15 or actually, according to this e-mail, both of  
16 them. They're the ones who noticed the  
17 misinformation, online, first; right?

18 MR. GARDNER: Objection to form.

19 BY MR. SAUER:

20 Q. Correct?

21 A. That's what -- that's what the  
22 e-mail appears to say, yeah.

23 Q. And they reached out, you know,  
24 proactively to Gwinnett County asking them to  
25 debunk it; right?

1 A. Yeah, they're just trying to get  
2 what was actually going on, yeah.

3 Q. Yeah, they say: We're tracking a  
4 social media post that's gaining traction very  
5 quickly. It's likely a misunderstanding, but  
6 being portrayed as a nefarious act. If you can  
7 clarify for us what is being shown, if it even  
8 happened, we can work with the social media  
9 platforms to try to have the post removed as  
10 misinformation; correct?

11 A. Yeah, that's what he wrote.

12 Q. And then Gwinnett County comes back  
13 with a -- a -- an explanation of the post;  
14 correct?

15 A. Yes.

16 Q. And that's forwarded to Twitter by  
17 CIS, along with their explanation; correct?

18 Well, actually, before they report  
19 it to Twitter they report it to you; right?  
20 Here's there's an e-mail that says --

21 A. Yeah.

22 Q. -- Brian and EIP --

23 A. Yes.

24 Q. Right? So Brian --

25 A. Yep.

1 Q. And EIP is Election Integrity  
2 Partnership; right?

3 A. Yep.

4 Q. And that's what CIS says, and they  
5 sent this to --

6 A. Yes.

7 Q. -- your e-mail, two CISA e-mails,  
8 their own e-mail and  
9 tips@2020partnership.atlassian.net; right?

10 A. Yep.

11 Q. So they sent this e-mail, where  
12 they say: Brian and EIP, to you, two CISA  
13 accounts, their own account, and  
14 tips@2020partnership.atlassian.net; right?

15 A. Yep.

16 Q. So it appears that that  
17 tips@2020partnership e-mail is an EIP e-mail;  
18 right?

19 MR. GARDNER: Objection, asked and  
20 answered, multiple times.

21 BY MR. SAUER:

22 Q. Does that refresh your memory?

23 A. I wouldn't say refreshes my memory,  
24 but it's going on CISA or CIS e-mail there, so  
25 it's probably a reasonable assumption to make.



1 Q. Then you forward this on, having  
2 received the report from CIS; right?

3 A. Yep.

4 Q. And then @Twitter reports back to  
5 you, and says, they labeled the tweet and are  
6 taking steps to limit trending; right?

7 A. Yes.

8 Q. What does that mean to take steps  
9 to limit trending; do you know?

10 MR. GARDNER: Objection, calls for  
11 speculation.

12 A. Yeah, I don't know. Twitter has a  
13 range of tools that they use. I couldn't  
14 possibly speculate on what they were doing here.

15 Q. Let's put Exhibit 12 back up.  
16 These are the interrogatory  
17 responses.

18 MR. GARDNER: Yeah, hold on one  
19 second, John. You said 12?

20 MR. SAUER: Yeah.

21 MR. GARDNER: Hold on one second.

22 MR. SAUER: Go to page 38.

23 THE WITNESS: 38.

24 MR. SAUER: Yeah, if you would.

25 THE WITNESS: Okay. I'm on page

1 38, John.

2 BY MR. SAUER:

3 Q. Oh, sorry, I'm on page 28. My  
4 mistake.

5 A. All right.

6 Q. 38 asks that here, you see where it  
7 says CISA, and it says: CISA responds that  
8 meetings taking place with the social media  
9 platforms relating to misinformation include,  
10 but are not limited to, and then there's a  
11 bullet list; right?

12 A. I think that is 38, not 28.

13 Q. Yeah, it should be on page 38?

14 A. Sorry. I thought you said 28. Let  
15 me get back down there.

16 Q. Oh, I meant I was mistaken.

17 A. Okay. So there's a table, am I  
18 looking below the table or above the table?  
19 Below the table?

20 Q. Yeah.

21 A. Got you. Okay.

22 Q. Okay.

23 A. I'm sorry, what am I looking for?

24 Q. Were you involved in identifying  
25 meetings between CISA and social media platforms

1 relating to misinformation in responding to  
2 discovery requests?

3 A. Yes, I believe I was.

4 Q. What meetings did you identify?

5 A. Certainly these, the recurring  
6 meetings listed here, that we talked about, the  
7 preparation meeting we talked about, going  
8 through the list, MDM, joint MDM working group,  
9 I think I missed -- those are the ones I would  
10 have identified.

11 Q. Start with the first one, first  
12 bullet point, a recurring meeting usually  
13 entitled USG industry meeting, which has  
14 generally had a monthly cadence; right?

15 A. Yep.

16 Q. And that is the one that you refer  
17 to as the sync meeting between industry and  
18 social media platforms; correct? I'm sorry,  
19 industry --

20 A. Right. Yes, that's correct.

21 Q. And you list there, I think seven  
22 or eight social media platforms, and the  
23 response, Google, Facebook, Twitter, Reddit,  
24 Microsoft, and then Verizon Media, Pinterest,  
25 LinkedIn and Wiki Media Foundation; correct?

1 A. Right, that's correct.

2 Q. And when you say this generally has  
3 a -- had a monthly cadence, in fact, far away  
4 from elections it was only quarterly, and then  
5 it became monthly close to elections, and became  
6 weekly before the 2020 election; right?

7 A. I would say from summer of 2018 to  
8 2020 they were -- to early 2020 they were  
9 quarterly. Sometime in 2020 they became monthly  
10 and then as we got closer to the election in  
11 2020 they became weekly.

12 Q. Why did they become weekly close to  
13 the election?

14 A. They were mostly just touch points  
15 in case anything kind of popped up. Those are  
16 much less formal than the monthly ones. We  
17 didn't have an agenda for those, just an  
18 opportunity for folks to share, if they had any  
19 questions or anything like that.

20 Q. What sort of stuff did folks share  
21 in these weekly touch point meetings?

22 A. So from a CISA perspective, we  
23 generally provide updates on any election  
24 security-related issues. So if -- you know, if  
25 there were any administrative kind of problems

1 that say we're having, speaking along those  
2 lines, the other federal partners, if they had  
3 any, again, kind of strategic, unclassified.  
4 Intelligence reporting that they felt was  
5 relevant, they might share that. And then the  
6 platforms, I don't know what they were sharing  
7 generally. I don't -- probably just general  
8 trends that they might be seeing on the  
9 platforms, but I don't recall specifically what  
10 they talked about.

11 **Q. And all these things that they**  
12 **share are related to election misinformation and**  
13 **misinformation on social media platforms?**

14 A. No. It also included cyber  
15 security, in fact, I would say most of it -- I  
16 wouldn't say most of it -- a lot of it was cyber  
17 security. And then there was a little bit on  
18 any physical threats that were occurring.

19 **Q. So that -- that's if someone was**  
20 **actually threatening poll workers, something**  
21 **like that?**

22 A. Correct.

23 **Q. And so in addition to physical**  
24 **threats, there were cyber security and issues**  
25 **related to misinformation and disinformation?**

1 A. Correct.

2 Q. Is anything else discussed in these  
3 meetings?

4 A. I mean, I think those are the  
5 main -- main topics that I recall.

6 Q. Was -- was the risk of hack and  
7 leak operations or hack and dump operations  
8 discussed in these meetings?

9 A. I don't -- I don't recall a  
10 specific incident of that, but it's definitely  
11 possible. It's a tactic that had been used in  
12 the past.

13 Q. Did you remember you raising  
14 concerns about hack and leak operations?

15 A. Me, personally, I don't recall  
16 myself raising that, but it's possible.

17 Q. How about -- how about Laura  
18 Dehmlow, did she ever raise that, discuss hack  
19 and leak operations?

20 A. Again, I don't know. It was a  
21 tactic that had been used globally, previously.  
22 So it wouldn't surprise me if there was some  
23 discussion of that somewhere in these meetings.

24 Q. Do you remember anyone on the  
25 government side discussing it?

1 A. Not specifically, no.

2 Q. How about on the industry side,  
3 anyone from the social media platforms  
4 discussing hack and leak operations?

5 A. Yeah, unfortunately, I just don't  
6 have that kind of recollection of conversations.  
7 So no, I don't specifically remember that.  
8 Again, it's possible, and I wouldn't be  
9 surprised.

10 Q. How about Elvis Chan, you know who  
11 he is; right?

12 A. I do.

13 Q. Did he ever -- do you remember him  
14 ever talking about hack and leak issues in these  
15 meetings in 2020?

16 A. Again, I don't have any specific  
17 recollection of that, but it's always possible,  
18 for sure.

19 Q. How about Matt Masterson?

20 A. Same answer, you know, it's  
21 possible, but I don't recall specific  
22 conversations.

23 Q. Let me e-mail you a couple more  
24 exhibits.

25 A. Sure.

1 Q. Do you know Yoel Roth is?

2 A. Yes, I know who Yoel Roth is.

3 Q. Do you know him personally?

4 A. Only in the fact that I've met him  
5 a couple times. He was at meetings, you know,  
6 some of these synch meetings he would be at.

7 Q. Were these meetings related to  
8 misinformation with CISA?

9 A. Again, these are regular sync  
10 meetings that we talked about, it's also I do  
11 recall we had some Twitter-only calls, as well,  
12 that he participated in, so again, it's general  
13 meetings would be of conversations.

14 Q. What was -- what was discussed in  
15 the Twitter-only meetings?

16 A. Similar, basic  
17 relationship-building stuff would be some of it,  
18 so, you know, just going and making sure we know  
19 who's who, and having conversations about, you  
20 know, just relationship-building sides. I also  
21 believe we had some briefings from them on some  
22 of their public reports, if I recall correctly,  
23 so things like that. There wasn't a ton of  
24 them.

25 Q. Is this public reporting related to



1 **misinformation and disinformation issues?**

2 A. Yeah, again, I don't know if that's  
3 what they called it, but that was kind of our  
4 interpretation of it. I think they used  
5 coordinated and in-authenticated or so, but I  
6 don't recall if Twitter -- if Twitter  
7 articulated it.

8 **Q. You would view those briefings in**  
9 **those bilateral meetings with Twitter as**  
10 **relating to misinformation and disinformation on**  
11 **social media?**

12 A. Yeah, some of that, and some of it  
13 I'm sure kind of talking him through how  
14 elections work, because a lot of education they  
15 weren't super familiar with the election  
16 administration, how they worked, and a different  
17 role and responsibility, you know, about  
18 elections. So again, we tried to educate as  
19 much as we could.

20 **Q. Were there bilateral meetings with**  
21 **other social media platforms, like this, where**  
22 **misinformation was discussed in any way?**

23 A. Yeah, again, generally, from a  
24 relationship-building standpoint, particularly  
25 early on in the process, we would meet -- we met

1 with the platforms just to talk about kind of  
2 what our role, what we would do, kind of how the  
3 relationship should act.

4 So just as an example, we could  
5 relate to the K-theoretical. You know, in those  
6 meetings we wanted to make sure that the  
7 platforms understood we would never ask them to  
8 undertake any specific actions. So we would  
9 reiterate that in all of our meetings. And, you  
10 know, that was something we continued throughout  
11 the process.

12 We would educate them on -- on  
13 elections, as I mentioned. We would talk to  
14 them a little bit about our resilience-building  
15 work, as I discussed. They would just kind  
16 of -- again, relationship-building type stuff,  
17 very general kind of conversations.

18 **Q. What you describe as the process,**  
19 **is that the process of, you know, referring**  
20 **disinformation concerns to them, that we've been**  
21 **talking about today?**

22 A. We did have conversations, but I  
23 think I was referring to the election processes,  
24 how the election processes worked.

25 **Q. You said early, when you said early**

1 in the process, you meant early in the election  
2 process?

3 A. Oh, yeah, sorry.

4 Q. You would have -- you had meetings  
5 with -- bilateral meetings with Twitter and  
6 Facebook and other social media companies?

7 A. Right. So in 2018 we didn't have  
8 any relationships with the platforms, at all.  
9 So in our initial stages of trying to build  
10 those relationships we would go meet with each  
11 platform one-on-one, just to make sure we could  
12 kind of talk to, understand what their concerns  
13 are, and then, you know, basic  
14 relationship-building stuff.

15 Q. Did those bilateral meetings happen  
16 in 2020, as well?

17 A. I would say they probably --  
18 probably had bilateral meetings in 2020. I'm  
19 not remembering any specific, off the top of my  
20 head, but I believe prior to starting the  
21 switchboarding work, in 2020, we had  
22 conversations with each platform individually.

23 Q. Those would be when you talk about  
24 what you would be doing in the switchboarding  
25 area; right?

1           A.    Yeah, kind of what we would be  
2           doing, and again, to reaffirm our position that  
3           we would never ask them to take any specific  
4           actions, that they should make decisions based  
5           on their term of service.

6           **Q.    So you're specifically talking**  
7           **about the fact that you would be sending them**  
8           **reports about disinformation during the election**  
9           **cycle?**

10          A.    Yeah, we would be forwarding them  
11          reports from different election officials, yeah.

12          **Q.    Just putting Exhibit 12 back up,**  
13          **here.**

14                    **Let me show you where in your**  
15                    **interrogatory responses you disclosed those**  
16                    **bilateral meetings with social media platforms**  
17                    **here in --**

18                    MR. GARDNER: Hold on. We're --  
19                    we're pulling 12 back up, John. Hold on.

20                    MR. SAUER: Page 38 to 39, it  
21                    actually goes onto 40.

22                    MR. GARDNER: Yeah, hold on. Whoa  
23                    whoa, whoa, whoa, yeah, almost there. You said  
24                    38, John?

25                    MR. SAUER: Page 38.

1 BY MR. SAUER:

2 Q. There's a list of five bullet  
3 points.

4 A. Okay. I'm sorry, what was your  
5 question?

6 Q. Can you show me where on this  
7 interrogatory response you disclosed, for  
8 example, bilateral meetings between CISA and  
9 Twitter or CISA and Facebook relating to the  
10 misinformation reporting that we've been talking  
11 about?

12 A. So I don't want to speak on behalf  
13 of whoever submitted the final product, but my  
14 assumption would be that they would be on the  
15 preparation meeting. But I'm not -- I'm not  
16 sure how they captured those in here.

17 Q. Were those the same as preparation  
18 meetings for the USG industry meeting?

19 A. I probably wouldn't consider them  
20 to be the same, but there's -- there are similar  
21 types of meetings.

22 (Exhibit No. 13 was marked for  
23 identification.)

24 BY MR. SAUER:

25 Q. Let's get Exhibit 13 back up.

1 Do you see this as a document filed  
2 before the FEC, entitled: Declaration of Yoel  
3 Roth?

4 A. Okay.

5 Q. And scrolling, have you seen this  
6 document before?

7 A. I have not.

8 Q. Scroll down to paragraph 11. Start  
9 with paragraph 10. Mr. Roth says in this  
10 declaration, he says, since 2018 I have had  
11 regular meetings with the office of the director  
12 of National Intelligence, the Department of  
13 Homeland Security, the FBI, and industry peers  
14 regarding election security; right?

15 A. Yep.

16 Q. Was this a description of the --  
17 the sync meetings that we talked about today,  
18 between US government and social media  
19 platforms?

20 MR. GARDNER: Objection, lack of  
21 foundation, calls for speculation.

22 BY MR. SAUER:

23 Q. Do you see that?

24 A. Yeah, I don't know what he's  
25 talking about, obviously I can't tell for

1 certain what he's talking about.

2 Q. No? Since 2018 has the Department  
3 of Homeland Security had regular meetings with  
4 social media platforms --

5 A. Yep.

6 Q. -- ODNI and the FBI?

7 MR. GARDNER: Objection, lack of  
8 foundation.

9 A. Yes.

10 Q. Yes, it has, because you've  
11 testified about them repeatedly today, so there  
12 obviously is a foundation, isn't there?

13 You have been personally involved  
14 in multiple meetings, these sync meetings,  
15 between USG and industry, and they involve seven  
16 or eight social media platforms, ODNI, the  
17 Department of Homeland Security, specifically  
18 CISA, and the FBI, didn't they?

19 A. We had regular meetings, as I  
20 talked about. Whether or not that is what Yoel  
21 is also talking about, here, I can't say. But I  
22 don't think that's a bad inference to make.

23 Q. Okay. Scroll down to paragraph 11:  
24 During these weekly meetings the federal law  
25 enforcement agencies communicated that they

1 expected hack and leak operations by state  
2 actors might occur in the period shortly before  
3 the 2020 presidential election, likely in  
4 October; do you see that?

5 A. Yes.

6 Q. Do you recall that kind of  
7 communication occurring in any of these sync  
8 meetings that occurred in 2020?

9 A. Again, I don't specifically recall.  
10 But as I said earlier, it's certainly possible,  
11 because it was a common tactic.

12 Q. But you don't remember any federal  
13 agencies talking about hack and leak operations  
14 in these meetings, but you don't dispute that it  
15 could have happened?

16 A. That's correct, yes.

17 Q. Okay. Next sentence, Mr. Roth  
18 says: I was told in these meetings that the  
19 intelligence community expected that individuals  
20 associated with political campaigns would be  
21 subject to hacking attacks, and that the  
22 material obtained through those hacking attacks  
23 would likely be disseminated over social media  
24 platforms, including Twitter; do you see that?

25 A. I do.



1           **Q. Do you recall that being**  
2           **communicated in any of these sync meetings?**

3           A. Again, it's -- I don't remember  
4           specifics, but it would not surprise me if this  
5           was discussed.

6           **Q. Next sentence, Mr. Roth says:**  
7           **These expectations of hack and leak operations**  
8           **were discussed throughout 2020.**

9                   **Does that ring a bell? Do you**  
10           **recall this being raised multiple times and**  
11           **repeatedly in these sync meetings?**

12           A. Again, it's the same response. I  
13           don't have specific memories of every item that  
14           was requested or very good memory of the  
15           conversations, in general. But I would  
16           definitely not be surprised if these were  
17           included in those conversations.

18           **Q. Okay. And then the very next**  
19           **sentence, spilling onto page 3, I also learned**  
20           **in these meetings that there were rumors that a**  
21           **hack and leak operation would involve Hunter**  
22           **Biden; do you see that?**

23           A. I do.

24           **Q. Do you recall any mention of Hunter**  
25           **Biden in any of these meetings with social media**

1 platforms?

2 A. I don't.

3 Q. So you don't know -- do you -- do  
4 you dispute that Mr. Roth remembers it  
5 correctly?

6 A. I mean, I have no basis to dispute  
7 or not dispute.

8 Q. Okay.

9 A. These aren't topics that CISA would  
10 be briefing on, so it's possible another agency  
11 did brief on them.

12 Q. How about the FBI, do you remember  
13 the FBI, Laura Dehmlow and Elvis Chan, saying  
14 anything about Hunter Biden during these  
15 meetings?

16 A. I don't.

17 Q. How about ODNI?

18 A. I don't, no.

19 Q. How about DOJ, national security  
20 division?

21 A. I don't, no.

22 Q. This is dated December 17th, 2020,  
23 so that would have been within a couple of  
24 months of these meetings, a month or two of the  
25 last meeting; is that right?

1           A.    I'm sorry, what was -- could you  
2           repeat that? I just want to make sure I  
3           understand what you're asking.

4           **Q.    I was just scrolling down to the**  
5           **fourth page of the document, where it's dated**  
6           **December 17th, 2020.**

7           A.    Oh.

8           **Q.    Do you see that?**

9           A.    Yep.

10          **Q.    So this declaration would be**  
11          **executed close in time to the meetings that are**  
12          **being discussed; correct?**

13          A.    Correct.

14                   MR. SAUER: I'm going to e-mail you  
15          Exhibit 14.

16                   MR. GARDNER: John, did you say 14?

17                   MR. SAUER: Exhibit 14, yeah, do  
18          you have that?

19                   MR. GARDNER: Yeah, we already have  
20          that, the deposition of Elvis Chan.

21                   MR. SAUER: Yeah. Sorry, guys.

22                                (Exhibit No. 14 was marked for  
23          identification.)

24          BY MR. SAUER:

25                   **Q.    This is the third page of this**

1 document.

2 A. Okay.

3 Q. There's an exchanges here where Mr.  
4 Chan is asked -- he refers to the federal law  
5 enforcement agencies, plural, in that sentence,  
6 do you see that answer, yes; do you see where  
7 that is?

8 A. Line four?

9 Q. Yeah.

10 A. Is that what you're referring to?  
11 Yeah, you're referring to the  
12 question at line four?

13 Q. Right.

14 A. Okay. Yeah, I see that.

15 Q. And Mr. Chan was asked the question  
16 on line eight, whether other federal law  
17 enforcement agencies, other than the FBI, talked  
18 about hack and leak operations; do you see that?

19 A. I do.

20 Q. And he says he doesn't think of any  
21 other federal law enforcement agencies, there at  
22 line 15. The only federal law enforcement  
23 agency I remember conveying our concern about  
24 hack and leak operations was the FBI; right?

25 A. That's his response, correct.

1 Q. And then he was asked, how about  
2 any other agency, not law enforcement. And he  
3 answered, as I mentioned, I believe CISA would  
4 have had the same concern as the FBI; right?

5 A. That was his response, yep.

6 Q. And I asked him: That was relayed  
7 through Mr. Masterson and Mr. Scully, I think  
8 you said, correct? And he answered, correct;  
9 right?

10 A. Okay. Yep.

11 Q. Do you remember either you or  
12 Mr. Masterson relaying a concern about hack and  
13 leak operations in those meetings?

14 A. I don't.

15 Q. Next page of the document, page  
16 222, fourth page of the PDF, you testify: I  
17 believe that the senior election official from  
18 ODNI would also flag -- flag that as a concern;  
19 correct?

20 A. Yes. That's what he says, yes.

21 Q. Do you remember anyone from ODNI  
22 raising a concern about hack and leak operations  
23 in these meetings?

24 A. Again, as I said in your previous  
25 questions, I don't recall specifics, but it

1 wouldn't surprise me if -- if they were  
2 mentioned.

3 MR. SAUER: I'm sending you Exhibit  
4 15 by e-mail.

5 (Exhibit No's. 15, 16 and 17 were  
6 marked for identification.)

7 MR. GARDNER: John, are you  
8 intending to screen share?

9 MR. SAUER: Yeah, I'm doing that  
10 right now.

11 MR. GARDNER: We're still waiting  
12 for the exhibit.

13 MR. SAUER: Sorry. I think I got  
14 my exhibits switched up. Yeah, here, I'm  
15 showing you exhibit -- I think it will be  
16 Exhibits 15, 16 and 17. You know, the one that  
17 I thought was 15 is 16, the one that I thought  
18 was 16 is 15, so I'm showing you Exhibit 16.

19 MR. GARDNER: So when we receive  
20 your e-mail do you want us to pull up the  
21 document marked 16?

22 MR. SAUER: Yeah, you should have  
23 received it already.

24 MR. GARDNER: Yeah, not yet.

25 MR. SAUER: There should be an

1 e-mail with 15, 16 and 17 all attached.

2 MR. GARDNER: Yeah, not yet.

3 MR. SAUER: Really? Well --

4 MR. GARDNER: Oh, here we go.

5 Do you want us to pull up 16 first?

6 MR. SAUER: Yeah.

7 MR. GARDNER: Okay. John, I have

8 15 here, and I got set up -- I see what's

9 happening. Hold on. Yeah, sorry.

10 MR. SAUER: It's a one-page e-mail,

11 it should be up.

12 MR. GARDNER: Yep. Yeah.

13 BY MR. SAUER:

14 Q. Here's a -- Mr. Scully, you see an  
15 e-mail here from Facebook to you and  
16 Mr. Masterson, as well as Allison Snell and  
17 Geoff Hale; correct?

18 A. I do.

19 Q. And there it indicates that there  
20 it's called today's industry statement; right?

21 A. Joint industry statement.

22 Q. Right. And they say -- and  
23 Facebook says to you, I wanted to ensure you had  
24 the statement we will look to release following  
25 today's meeting; right?

1 A. Correct.

2 Q. And then, under the joint industry  
3 statement, it talks about how there are these  
4 meetings that have been going on; right?

5 A. Yes.

6 Q. And then it says -- the majority of  
7 the statement says: At today's meeting we  
8 specifically discussed three things; right?

9 A. Yes.

10 Q. And the second one of those says:  
11 Ways to counter targeted attempts to undermine  
12 election conversation before, during, and after  
13 the election; right?

14 A. It does.

15 Q. And the industry statement goes on  
16 to say: This includes preparing for possible  
17 so-called hack and leak operations, attempted to  
18 use platforms and traditional media to amplify  
19 unauthorized information drops; correct?

20 A. Correct.

21 Q. Does that -- and so the industry  
22 prepared a public statement saying that hack and  
23 leak operations were discussed at one of these  
24 meetings; correct?

25 A. Correct. Yes.



1 Q. Does that refresh your memory, at  
2 all, about hack and leak operations being raised  
3 at these sync meetings in 2020?

4 A. Again, I don't have any specific  
5 recollections of the conversations. But as I  
6 said a few times, now, it doesn't surprise me  
7 that they would discuss the common tactic used  
8 globally.

9 Q. Were you aware of any pending  
10 investigations, at that time, into possible  
11 hack -- actual possible hack and leak  
12 operations?

13 A. No.

14 Q. I'm showing you what should be  
15 Exhibit 15.

16 MR. GARDNER: Got it.

17 THE WITNESS: Okay.

18 BY MR. SAUER:

19 Q. And here's an e-mail from Lauren  
20 Protentis to people at Facebook and CISA, that  
21 refers to the prep USG industry called monthly,  
22 in the subject line; correct?

23 A. Yes, correct.

24 Q. And I think you testified earlier  
25 that Facebook was kind of the point for the

1 industry. And so there would be a preparatory  
2 meetings between CISA and Facebook to kind of  
3 set the agenda for the big monthly meeting that  
4 involved all the platforms and at least four  
5 agencies; right?

6 A. That's correct, yeah.

7 Q. Okay. Here it says, among other  
8 things, industry prompts, themes, narratives,  
9 approaches you anticipate for races you think  
10 will be targeted, right, is number two?

11 A. Yes.

12 Q. Okay. What's that talking about,  
13 are they asking that industry to report back on  
14 what themes and narratives on social media they  
15 anticipate may happen in certain election races?

16 A. So I'm not -- I'm not sure what,  
17 specifically, they were talking about here.  
18 It's possible they were trying to understand if  
19 they were particularly they were being targeted  
20 by foreign actors, but I don't know, that's --

21 Q. How about themes and narratives?

22 A. Yeah, I think that would be  
23 pretty --

24 Q. Go ahead.

25 A. I think that would be the same kind

1 of idea. Again, as I mentioned earlier, in a  
2 lot of these calls the intelligence community  
3 would provide kind of high-level assessments of  
4 unclassified reporting that they had done.

5 **Q. What does industry prompts mean?**

6 A. Generally speaking, it would be the  
7 questions that industry had for government.

8 **Q. So industry --**

9 A. For --

10 **Q. Go ahead.**

11 A. Actually, let me rephrase. Sorry.

12 I think in this case it's --

13 it's -- I'm not sure, that's how I would have  
14 interpreted it, but based on where it is in the  
15 agenda I'm not sure that's what Warren meant.

16 **Q. In other words, these questions of**  
17 **government for industry say, hey, social media**  
18 **platforms tell us what themes, narratives,**  
19 **approaches you're anticipating for the upcoming**  
20 **election?**

21 A. No, my -- my interpretation of this  
22 is that it's industry questions for government,  
23 because the government portion of the agenda.  
24 So industry, if possible, would like to hear  
25 government's perspective on these questions.

1 Q. Did government share that with the  
2 social media platforms in these meetings? Did,  
3 you know, the federal agencies talk about what  
4 themes and narratives and approaches they  
5 anticipated on social media for election races?

6 MR. GARDNER: Objection, compound.

7 THE WITNESS: Yeah, can you just  
8 kind of break that question down for me?

9 BY MR. SAUER:

10 Q. In the actual meetings did the  
11 federal agencies provide information to the  
12 social media platforms about the themes and  
13 narratives they anticipated seeing on social  
14 media for particular races, election races?

15 A. I don't think it was ever broken  
16 down by particular races. I think there were --  
17 again, there was intelligence. If there's  
18 intelligence that was unclassified they could be  
19 shared about, targets and things like that, the  
20 intelligence community would share that.

21 But generally speaking, I don't  
22 think that we would necessary get down to the  
23 individual race level, but again, I'm not -- I  
24 don't have a memory of every specific item that  
25 was discussed.

1           Q.    How about do you remember themes  
2           and narratives being discussed, like, hey, we  
3           expect people to be, you know, talking about --  
4           expect, you know, social media postings to  
5           reflect this theme or that narrative?

6           A.    So I think there are two components  
7           to this one. I believe there are some  
8           discussion about would we have seen historically  
9           in the past, and may see going forward. So --  
10          so I believe there might have been some  
11          discussion around that.

12                    And then if -- again, if the intel  
13           communities had reporting talked about foreign  
14           actor efforts, they would share those.

15                    I don't recall, specifically, what  
16           was discussed. So I -- I don't know if -- what  
17           level of detail, if any, they got down to in  
18           those conversations.

19                    And I'm not even -- to be honest,  
20           I'm not even sure if I attended this meeting. I  
21           think I either just got back from my detail or  
22           it was right before I got back to my detail, so  
23           I'm not sure I attended this one.

24           Q.    I'm going to share Exhibit 17.

25           A.    Okay.

1 Q. And this is a collection of  
2 e-mails, again.

3 Here on the first page, in April of  
4 2022, this year, Lauren Protentis is sharing the  
5 agenda for one of these USG sync meetings. And,  
6 among other things, she says: One-pager  
7 reminder; do you know what she's talking about?

8 A. Yeah, she -- we had asked industry  
9 to provide a one-page summary of their content  
10 moderation rules that we could share with  
11 election officials.

12 Q. What's the purpose of that, a  
13 one-page summary of their content moderation  
14 rules?

15 A. So we -- we would receive a lot of  
16 questions from election officials about how  
17 different platforms made decisions about their  
18 terms of service. And we thought this was a way  
19 to help the platforms be more transparent with  
20 election officials. So we asked them to just  
21 put together kind of a one-page summary.

22 Q. A one-page summary of basically  
23 what their content moderation policies were as  
24 applies to election misinformation?

25 A. Yeah, that we could share with

1 election officials.

2 Q. I take it, then, the election  
3 officials when they see something on social  
4 media that they view as disinformation or  
5 misinformation would be educated on whether or  
6 not it violates that platform's policy; is that  
7 right?

8 A. I'm not sure that was the full  
9 expectation, but I think it was just to try to  
10 provide some transparency and some understanding  
11 of how the platforms make a decision.

12 Q. And why is it useful? I take it  
13 this was your idea, CISA's idea, not -- it  
14 wasn't something that the election officials  
15 have asked for?

16 A. To be honest, it asks of maybe  
17 before I returned, so I'm not entirely certain,  
18 but I suspect it was some combination of  
19 election officials asking. We got a lot of  
20 questions over the years about that, and us  
21 just, you know, raising it with the platforms  
22 the way they're trying to help the election  
23 officials.

24 Q. Jumping ahead, 15743, should be on  
25 the 7th page of the PDF, there's a discussion in

1       **the April --**

2                   MR. GARDNER: Are you at that now?

3                   THE WITNESS: Sorry, I just  
4       accidentally got out. I'm going to the page. I  
5       think I'm there.

6       BY MR. SAUER:

7                   **Q.     There's a discussion, a bullet**  
8       **point in the agenda for the August 2020 USG**  
9       **industry meeting of election-day coordination.**

10                   Do you know what -- what that was  
11       discussed under that?

12                   A.     Yeah, and just to be clear, you  
13       know, we just jumped from 2022 back to 2020;  
14       right?

15                   **Q.     Yeah.**

16                   A.     Okay. Yeah, so CISA regularly set  
17       up an operation center on election day, around  
18       the election. And the platforms and some of the  
19       other agencies do the same. But I think it was  
20       just a conversation about how all the different  
21       organizations were going to be managing on  
22       election day.

23                   **Q.     What is the nature of a -- what is**  
24       **CISA's election day operation do, does it**  
25       **receive disinformation reports?**



1           A.     It's more of a -- so just taking a  
2     step back, right, essentially what CISA does is  
3     it invites key stakeholders to CISA to  
4     facilitate information sharing about what's  
5     going on within the elections.

6                     Most of it is cyber related, but  
7     the NAV and NAFTA that we talked about earlier  
8     were there, and so if they heard reporting up  
9     through their members, they might mention it.

10                    Generally speaking, you might  
11    have -- in 2020 it was a little different,  
12    because of COVID. But generally speaking, we  
13    would have somebody from our team there who we  
14    would have a team kind of working on the chats.

15                    And so the switchboard reporting  
16    might come in and in 2018, for example, our guy  
17    was sitting in the room, in 2020 I think I was  
18    the only one in the room, maybe one other from  
19    our team. And then they would -- you know, so  
20    that's -- I don't know if that helps clarify. I  
21    think I just talked in mode right there.

22                    **Q.     When you say in the room, is there,**  
23    **like, a physical location where CISA and NASED**  
24    **and NASS and social media platforms all have**  
25    **people or what room are we talking about?**

1           A.    Yeah, so in 2020, CISA had a room  
2           where we had some of our stakeholders attend in  
3           person. I don't have a full list of who was  
4           there. It was obviously not substantial, due to  
5           COVID restrictions. But we would have federal  
6           partners, and we have NASS and NASED there.

7                        I don't know who else was there,  
8           but I believe there was a couple other, you  
9           know, maybe election security vendors, folks  
10          like that, just to facilitate information  
11          sharing in case an incident occurred.

12                   **Q.    Who were the federal partners?**

13          A.    I don't -- I don't believe in 2020  
14          we had too many in the room, but CISA's watch  
15          center operations for CISA central I talked  
16          about earlier, they're our liaisons for many of  
17          the different agencies, and then we had  
18          connectivity with FBI, DOJ, NEI, I&A, things  
19          like that. Again, 2020 all you need due to the  
20          pandemic.

21                   **Q.    And part of what happens in this**  
22                   **election-day operation is that NASED and NASS**  
23                   **may receive misinformation reports from their**  
24                   **members and report them up to you guys; right?**

25          A.    Generally speaking, it would --

1 they would handle them themselves, with the  
2 platforms, but I'm sure there were examples of  
3 where they sent it to us.

4 Q. And then would you guys perform the  
5 same misinformation routing function and pass  
6 that along to the platforms?

7 A. Yeah, correct.

8 Q. Okay. This happened again in 2022,  
9 was there an election-day operation?

10 A. It was an election operation center  
11 in 2022. We didn't do switchboarding in 2022,  
12 as we discussed earlier.

13 Q. You say you didn't do  
14 switchboarding in 2022, did you relay --

15 A. Correct.

16 Q. -- misinformation or disinformation  
17 concerns to social media platforms at any time  
18 during the 2022 election cycle?

19 A. Not that I recall, no.

20 Q. How did the state and local  
21 election officials relay those concerns to the  
22 social media platforms, did they do a --

23 A. Yeah, my understanding was  
24 two-fold, one, I think some of the platforms  
25 developed a little more robust infrastructure to

1 engage with election officials, themselves. And  
2 then I also believe that CIS was up and running,  
3 but I'm not certain what -- kind of how it all  
4 worked.

5 Q. So you believed that CIS continued  
6 to receive disinformation/misinformation reports  
7 from state and local election officials during  
8 the 2022 election cycle, and relay them directly  
9 to social media platforms?

10 A. Yeah, I'm speculating a bit on  
11 that, because I'm not particularly familiar with  
12 what they actually did in 2020, but that was the  
13 general understanding I had.

14 Q. Did they copy you on those reports,  
15 like they were doing in 2020?

16 A. They were not, no.

17 Q. Why not? Did you tell them not to?  
18 Did you say: Don't copy us on these or did they  
19 just stop?

20 A. Yeah, we discussed earlier, CISA  
21 didn't -- was not doing switchboarding in 2022,  
22 so there's no reason for them to copy us.

23 Q. And did you tell --

24 A. But I --

25 Q. Go ahead.

1           A.     So I didn't have a conversation,  
2     myself, with CIS about it, so I'm not sure who  
3     told them not to do it.

4           **Q.     Turning back to the 2022 election**  
5     **day operation, was that another case where CISA,**  
6     **NASED, NASS, and other federal agencies all had**  
7     **representatives in one room?**

8           A.     I -- I think there was some federal  
9     representative there, like I said, most of that  
10    would -- would be in the ops center. There were  
11    other nongovernment partners there, like -- like  
12    I said, like the -- the vendors, election  
13    security, election system vendors and folks like  
14    that.

15          **Q.     What -- what's the ops center?**

16          A.     That's essential, that's kind of  
17    the 24/7 situational awareness that CISA runs.  
18    And my understanding is that it has liaisons  
19    from across the federal agencies.

20          **Q.     And were you there at the -- at the**  
21    **ops center in 2022 election day?**

22          A.     So the room we would be in would be  
23    a separate room. We wouldn't actually be on the  
24    ops center floor. We called it a situational  
25    awareness room.

1 Q. On election -- were you there?

2 A. I was in the situational awareness  
3 room on election day in 2022, yep.

4 Q. Any misinformation or  
5 disinformation concerns arise on election day in  
6 2022?

7 A. I don't think there was too much.  
8 I'm not recalling specific incidents. I would  
9 imagine the two were, but I don't think there  
10 was very much, if there was.

11 Q. What happened?

12 A. I'm sorry, that's not very clear.  
13 I just don't recall if there's  
14 anything specific. I have a general sense that  
15 there were a couple of items, but I don't think  
16 there was very much.

17 Q. What happened to the ones that did  
18 occur or that did arise, did they get routed to  
19 different platforms?

20 A. No, I think it -- no, if any of  
21 those were mentioned, I think it was just in  
22 general conversation of what might be happening,  
23 but we didn't have anything on social media  
24 platforms.

25 Q. Did NASED and NASS route things to

1       **social media platforms?**

2               A.    I don't -- I don't know for  
3       certain. I would -- I would guess they did.

4               Q.    **Jumping ahead in Exhibit 17, page**  
5       **14545, it's page 12 of the PDF, and here's an**  
6       **agenda from one of these sync meetings from July**  
7       **of 2022; do you see that?**

8               A.    Is it 14545?

9               Q.    **Yeah, page 12 of the PDF.**

10              A.    Just making sure. Sorry, it's  
11       weird how it shows the pages here. Yeah, okay.  
12       Yep.

13              Q.    **And then Lauren Protentis, here, is**  
14       **circulating an agenda for a sync meeting;**  
15       **correct?**

16              A.    This looks like it's for a prep  
17       meeting.

18              Q.    **Prep meeting? Okay.**

19                    **And then here in item four, it**  
20       **says: CISA elections infrastructure risks,**  
21       **Scully; correct?**

22              A.    Yep.

23              Q.    **So is that referring to the plan**  
24       **that you -- and do you have a briefing on**  
25       **election infrastructure risks at the big sync**

1 meeting?

2 A. Yeah, I believe normally Geoff Hale  
3 would do that, I believe this meeting Geoff was  
4 going to be unavailable, so they asked me to  
5 cover the election infrastructure portion of the  
6 agenda.

7 Q. Now, what you said about them, what  
8 does that mean, election infrastructure risks,  
9 does that refer to informational infrastructure?

10 A. No, that's -- again, that's kind of  
11 the broader understanding of how elections  
12 function, so the systems, physical security,  
13 things like that. It would just be an update on  
14 kind of where things stand across kind of the  
15 broader election infrastructure community.

16 Q. Below that, item six, it says:  
17 FBI, domestic, adversarial actor update, down  
18 below; do you see that?

19 A. I do.

20 Q. Do you recall Laura Dehmlow giving  
21 a briefing at that meeting you were at about a  
22 domestic adversarial actor?

23 A. I don't, and I -- I -- if I recall  
24 correctly, and I don't know if you have the  
25 actual agenda for the meeting, I think the --



1 that changed.

2 Q. Oh, you don't think she gave  
3 that -- that -- that briefing?

4 A. I don't believe so, no.

5 Q. What kind of domestic adversarial  
6 actors is the FBI's foreign influence task force  
7 concerned about?

8 A. I don't know.

9 Q. Let's jump ahead to page 7599.

10 MR. GARDNER: John, before we go  
11 on, we've been going about two hours, again. I  
12 think now would probably be a good time for a  
13 break.

14 MR. SAUER: I just got a few more  
15 questions about this document. Can you keep  
16 going for a couple more minutes.

17 MR. GARDNER: Sure, we can do that.

18 BY MR. SAUER:

19 Q. Let's just -- here, 7599.

20 A. What page are we on?

21 Q. That is page 16 of the PDF?

22 A. Okay.

23 Q. Do you see here on the bottom half  
24 of the page, on July 1st, 2020, Facebook sends  
25 e-mail to you and Matt Masterson, Matt and

1 Brian, thank you so much for the outreach on our  
2 next sync; right?

3 A. Yep.

4 Q. And then she gives a proposed  
5 agenda for a meeting that she proposes having on  
6 July 15th of 2020; correct?

7 A. Yes.

8 Q. And then, in that agenda, there's  
9 an item here, under number two, that says:  
10 Hack/leak and USG attribution speed/process; do  
11 you see that?

12 A. Yep.

13 Q. What was that referring to?

14 A. I -- I don't recall. You know, I  
15 would have to speculate based on what it says  
16 here.

17 Q. So you don't remember hack/leak  
18 being put on the agenda for one of these  
19 meetings?

20 A. Again, as I said earlier, I don't  
21 remember all the agenda items on the meetings or  
22 specific discussion points. But I'm not  
23 surprised that it's on here, no.

24 Q. Do you know why Facebook would have  
25 put that on?

1 MR. GARDNER: Objection, calls for  
2 speculation.

3 BY MR. SAUER:

4 Q. If you know.

5 A. I don't know.

6 Q. And then what is --

7 A. I mean, again --

8 Q. Go ahead.

9 A. Sorry, just as I said, you know, a  
10 few times, right, it's not surprising, it was a  
11 common tactic that was used globally. But I  
12 don't know why they -- if there was a specific  
13 reason that they put it on here.

14 Q. What -- how about that, in the  
15 second half of that line, USG attribution  
16 speed/process; right? Do you know what that  
17 means?

18 A. I don't, CISA doesn't do  
19 attributions, so I'm not sure what that could be  
20 related to.

21 Q. Attribution, when you say CISA does  
22 not do attribution, what does that mean?

23 A. Well, the way I would look at  
24 attribution would be attributing specific actors  
25 to something.

1 Q. That was --

2 A. In the MDM context CISA does not do  
3 attribution.

4 Q. So attribution is figuring out who  
5 is the actual source of the social media  
6 posting?

7 A. I mean, if you're talking about a  
8 social media posting, that would be attribution.  
9 If you're talking about hack and leak, I assume  
10 that would be known as the attribution to who  
11 the hacker and leaker was.

12 Q. So this, then, could be a  
13 discussion of -- you know -- and by the way,  
14 this is listed there under 40 minutes deep dive  
15 topics; right?

16 A. Mm-hmm.

17 Q. Do you know if you participated in  
18 that July 15th, 2020 meeting?

19 A. I would imagine I did, but I -- you  
20 know, I would have to go back and look at my  
21 calendar. I don't know for certain.

22 Q. You don't know -- sorry.

23 You don't know about whether there  
24 was a deep dive on hack/leak and USG  
25 attributions, the process?

1           A.    I don't know for certain. I mean,  
2           I would have to go back. Do you have the actual  
3           agenda that we used for the meeting or just the  
4           proposed one by -- by Facebook?

5           **Q.    No, let me ask you this: I take it**  
6           **you -- you interpret, in the context of hack and**  
7           **leak, USG attribution, USG is United States**  
8           **government; right?**

9           A.    Yeah, that's what I would assume it  
10          is.

11          **Q.    Attribution, I take it, is having**  
12          **the USG, the government, figure out who did the**  
13          **hack and the leak; right? That's what**  
14          **attribution means in this context?**

15          A.    Assuming I was connected to hack  
16          and leak, I obviously don't know what this is  
17          specifically referring to, but if I were reading  
18          that bullet point that's how I would read it,  
19          that the attribution was USG attributing a hack  
20          and leak.

21          **Q.    Okay. And then the question is**  
22          **how -- how fast speed and how USG would go about**  
23          **doing it; right, speed/process?**

24          A.    Again, that's what the agenda says.  
25          I don't know exactly what that means.

1 MR. SAUER: Let's take a break  
2 there.

3 MR. GARDNER: 10 minutes good?

4 MR. SAUER: Yeah. How long have we  
5 been on the record.

6 THE VIDEOGRAPHER: The time is now  
7 3:34 p.m. We are off the record.

8 (Recess.)

9 THE VIDEOGRAPHER: The time is now  
10 3:50. We are back on the record.

11 MR. SAUER: Before we go back to  
12 questioning, I'm formally requesting, on the  
13 record, a supplementation of the document  
14 production directed to CISA custodians. If you  
15 look at those pages where the key custodians are  
16 disclosed, we've had testimony today that that  
17 list of custodians at ESI should have been  
18 searched, should have included the five names  
19 that the witness has testified to today, Chad  
20 Josiah, Rob Schaul, Adam Zaheer, John Stafford  
21 and Pierce Lowary.

22 And, in fact, I think it's  
23 astonishing that four of those names are  
24 specifically identified as copied on e-mails  
25 from the key custodians, but whose ESI was not

1 searched.

2 So I request supplementation by  
3 tomorrow, which is the close of fact discovery.  
4 We were entitled to that going back to August.  
5 And this is the first time we've heard about  
6 this, one day before the close of discovery.

7 So I'm asking for those e-mails  
8 from those custodians, including their  
9 communications with social media platforms, and  
10 it now appears there were communications with  
11 the EIP, potentially, those be produced by  
12 tomorrow.

13 MR. GARDNER: I understand your  
14 request. We'll take it back.

15 MR. SAUER: Thanks.

16 (Exhibit No. 18 was marked for  
17 identification.)

18 BY MR. SAUER:

19 Q. Let's go to Exhibit 18, it should  
20 be in your e-mail.

21 MR. GARDNER: Yeah, hold on one  
22 second.

23 BY MR. SAUER:

24 Q. This document is another one of  
25 these collective exhibits of a bunch of CISA

1 e-mails involving you.

2 If you look at the first page, in  
3 the middle, here, it indicates there's reporting  
4 that you are forwarding from the state  
5 department's global engagement centers about  
6 disinformation on YouTube, and you're forwarding  
7 it onto -- to social media platform; do you see  
8 that?

9 A. Yes.

10 Q. Yeah. Let me ask this: What role  
11 does the state department's global engagement  
12 center have in addressing misinformation and  
13 disinformation on social media?

14 A. I don't know what the specific  
15 authorities are.

16 Q. Do you know what they do,  
17 generally?

18 A. Yeah, but also, just to be clear,  
19 that this e-mail is regarding a State Department  
20 employee that was targeted overseas, I believe.  
21 So I -- to answer your -- to answer your  
22 question, I believe they -- they have a mandate  
23 to deal with information operations overseas.

24 Q. Do you interact with them, at all,  
25 in your MDM team activities?



1 A. Yes.

2 Q. How do you interact with them?

3 A. In a couple ways. So one, they do  
4 a lot of reporting on what they're seeing  
5 overseas, particularly as it relates to actions.  
6 So it's a good source of understanding tactics  
7 and things like that, that are occurring  
8 overseas.

9 We often see what happens overseas  
10 end up showing up domestically. So it's a good  
11 source of information for that.

12 They also have a tech demo program  
13 that they run, where they bring in different  
14 tech companies that work in the information  
15 operations space. So we'll go -- we have  
16 members of the team that will go and watch some  
17 of the demo.

18 So I think those are the two main  
19 ones. We -- trying to think if there's others.

20 Q. Do you know George Beebe,  
21 B-e-e-b-e?

22 A. Do I know George? I'm sorry, could  
23 you spell that again?

24 Q. B-e-e-b-e.

25 A. The name does not sound familiar.

1           **Q. Do you know if the GEC was involved**  
2           **in the Election Integrity Partnership in any**  
3           **way?**

4           A. I don't. I know you showed me a  
5           document earlier, that they were listed, but I  
6           don't know what they did.

7           **Q. Okay. Second page, here, where**  
8           **this lists information report, you said -- it**  
9           **indicates, in the last sentence there, the**  
10          **journalist tells me there's a YouTube channel**  
11          **run by Americans falsely claiming that this**  
12          **diplomatic officer is patient zero for COVID-19;**  
13          **correct?**

14          A. I'm sorry, what page are you on?

15          **Q. Second page of the PDF.**

16          A. Okay. Yes, that's what the e-mail  
17          says.

18          **Q. So you said -- well, maybe**  
19          **overseas, it looks like the thing they're**  
20          **challenging is something posted by Americans;**  
21          **correct?**

22          A. I -- I don't know. I mean, that's  
23          just a YouTube channel run by Americans, that's  
24          what they say, yeah.

25          **Q. You forward this onto him; right?**

1 A. I believe that's true, yes.

2 Q. Scrolling down to page 10718 -- by  
3 the way, did you flag these accounts? If you  
4 look here on the 11th page of the PDF for a  
5 section --

6 A. Sorry, page 11 of the PDF?

7 Q. Yeah, here there's a screen shot of  
8 unofficialcogov, and the Twitter handle, says:  
9 DM us your weed store location, open  
10 parentheses, hoes be mad, but this is a parody  
11 account; correct?

12 A. It appears I forwarded it to  
13 Twitter, yes.

14 Q. Okay. And then that was the only  
15 one, and the next page there's one you forwarded  
16 to Twitter that says: Smoke, weed, erry day, I  
17 think they mean every day. The official  
18 (unofficial) Twitter account of the State of  
19 Colorado; right?

20 A. Yeah, it seems to be part of the  
21 same e-mail in Colorado.

22 Q. Those two accounts you forwarded to  
23 Twitter, you forward those to Twitter for  
24 consideration; correct?

25 A. Yeah.

1 Q. And then, sorry, moving back a  
2 little bit of the document, I apologize, on the  
3 9th page there's an e-mail on September 25th of  
4 2020, from you to Twitter, saying, good morning,  
5 do you all have five minutes for a quick call  
6 today. I'd like to give you a quick update on  
7 our reporting process this year. Do you know  
8 what that was about?

9 A. I don't --

10 Q. It looks like --

11 A. -- know specifically what it's  
12 about, no.

13 Q. It looks like the specific subject  
14 you mentioned was: Election disinfo reporting;  
15 correct?

16 A. Let me scroll down. Do you have  
17 the rest of the e-mail chain? Obviously it  
18 appears to be a reply to something. Am I  
19 missing something, here?

20 Q. Well, this is all we've got. It  
21 says --

22 A. Oh, there's no -- there's no  
23 header, again.

24 Q. But -- but Twitter's response to  
25 you, says: Re: Election disinfo reporting?

1 A. Yeah.

2 Q. Okay. Do you know -- do you  
3 remember having a call with them about your  
4 process reporting election disinformation on  
5 that date?

6 A. I don't.

7 Q. Next page, 9703, tenth page of the  
8 PDF, there's an e-mail from Twitter to you and  
9 Matt Masterson, in September of 2020, where it  
10 says: Hi Matthew and Brian, hope you're doing  
11 very well. We want to give you an update today.  
12 We're updating our civic integrity policy. Our  
13 existing policy does such and such, and it says,  
14 starting next week we will label or remove false  
15 or misleading information intended to undermine  
16 public confidence in an election or other civic  
17 process; right?

18 A. Yep.

19 Q. Do you know why they gave you this  
20 report?

21 MR. GARDNER: Objection, calls for  
22 speculation.

23 A. Yeah, I don't know why they  
24 specifically -- it looks like there's ways to  
25 public information about it, so as I mentioned

1 earlier, sometimes they would -- they're putting  
2 things out publicly they would just give us a  
3 heads up.

4 Q. Now, have you ever asked them to  
5 give you a heads up or Matt Masterson ask them  
6 to give you a heads up about changes in their  
7 content moderation policies?

8 A. Not that I recall.

9 Q. Page 8519, sorry, I'm in the wrong  
10 spot on the document.

11 Let me ask you this: Do you  
12 remember sharing a -- with Facebook, a  
13 disinformation report about CISA and Director  
14 Krebs, does that ring a bell, where the  
15 disinformation was disinformation about your own  
16 agency?

17 A. I don't recall that, specifically,  
18 no.

19 Q. Here it is, 19th page of the PDF.

20 A. 19?

21 Q. Yeah, page 19 of the PDF.

22 A. Okay.

23 Q. And it says: Good afternoon -- you  
24 sent an e-mail on November 5th of 2020 to  
25 Facebook, saying, good afternoon Facebook,

1       **wanted to share this disinfo report about CISA**  
2       **and Director Krebs; do you know what that was**  
3       **about?**

4             A.    I don't.

5             Q.    **And your second --**

6             A.    I don't recall.

7             Q.    **The second line says: IG disinfo**  
8       **report; do you know what IG means?**

9             A.    It appears, based on the link in  
10       the e-mail, that it was referring to Instagram.

11            Q.    **By you don't remember -- you don't**  
12       **remember a specific -- anything specific**  
13       **relating to Director Krebs, do you?**

14            A.    No, I don't.

15            Q.    **Let's scroll ahead a few pages, to**  
16       **10394.**

17                    **Well, let me ask this: Do you**  
18       **remember disinformation about Director Krebs**  
19       **circulating in that timeframe, just after the**  
20       **2020 election?**

21            A.    I recall that he was named on an  
22       Iranian-driven enemies of the people list.  
23       Beyond that, I don't -- I don't recall any other  
24       specific MDM related to the director, no.

25            Q.    **Okay. Scroll down to the 22nd page**

1 of the PDF.

2 A. Okay. Okay.

3 Q. Do you see here, you sent an e-mail  
4 to Facebook on November 10th, 2020, saying:  
5 Good morning, Director Krebs is particularly  
6 concerned about the hammer and scorecard  
7 narrative that is making the rounds; do you see  
8 that?

9 A. Yep.

10 Q. Do you know what that was, the  
11 hammer and scorecard narrative?

12 A. If I remember correctly, it was  
13 something about the NSA, and maybe a different  
14 federal agency, conspiring to change votes or  
15 something along those lines. Like there's new  
16 technology that the NSA developed. I forget the  
17 specifics of the narrative, itself, but it's  
18 something along those lines.

19 Q. So this is a narrative on social  
20 media suggesting that the federal government is  
21 engaging in intellectual or sort of election  
22 interference in some way?

23 A. I think it could have been social  
24 media, it could have been other media. I'm not  
25 sure what I was referring to when I said making



1 the rounds. I don't recall.

2 Q. Okay. Well, your next sentence  
3 says: Wanted to see if you all, meaning  
4 Facebook, have been tracking this narrative and  
5 if there's anything you can share around  
6 amplification; right?

7 A. Yep.

8 Q. What does amplification mean?

9 A. If a particular narrative is being  
10 amplified.

11 Q. So, in other words, you wanted to  
12 know -- you're asking Facebook to tell you  
13 whether or not that narrative is being amplified  
14 on its platform?

15 A. Correct. That's how I read that,  
16 yeah.

17 Q. Okay. And then Facebook responds  
18 by saying: Our teams are actively -- actively  
19 monitoring developments on this at this time and  
20 to the extent you or USG have information about  
21 confirmed misinformation or other information of  
22 note, we absolutely welcome that; correct?

23 A. Yep, that's what they wrote.

24 Q. And they follow up by saying:  
25 Wanted to follow up on the below to say that our

1 teams have confirmed that we have third-party  
2 fact checker verification that the "hammer and  
3 scorecard" narrative is false; right?

4 A. Yes, that's what they say.

5 Q. And they go on to report to you:  
6 Our systems are labeling and downranking the  
7 contents as identified; correct?

8 A. Yes.

9 Q. Is that consistent with other  
10 e-mails, where they report back to you on how  
11 they've taken action against a content that you  
12 have flagged?

13 A. Yeah, generally consistent, I  
14 think.

15 Q. Let's jump ahead to the 10390, that  
16 is going to be page 24 of the PDF, and here at  
17 the bottom of the page you sent the very same  
18 e-mail to Twitter, as well; right?

19 A. Yep.

20 Q. Director Krebs is very concerned  
21 about the hammer and scorecard narrative, and  
22 I'm wondering if you have been tracking this  
23 one, if there's anything you can share in terms  
24 of sharing and amplification; correct?

25 A. Yeah, that's what I wrote.

1 Q. The usual context says: We have  
2 been tracking this issue. I will allow Yoel to  
3 follow up with detailed information; right?

4 A. Yes.

5 Q. And that's Yoel Roth; right?

6 A. I believe so, yeah, that's -- let's  
7 see, yep.

8 Q. He was then the chief content  
9 modulation officer for Twitter, right, ahead of  
10 their trust and safety team?

11 A. I don't recall what his title was,  
12 but he certainly was in charge of some trust and  
13 safety, safety stuff.

14 Q. Trust and safety, that means  
15 enforcing content moderation policies; right?

16 A. I suspect that's one of the  
17 responsibilities.

18 Q. He comes back to you with a kind of  
19 detailed report here at the top of the page  
20 about what Twitter's been doing on this, he  
21 says, we've been tracking the hammer/scorecard  
22 issue closely, particularly since Director  
23 Krebs's tweet on the subject, which is pretty  
24 unambiguous as debunks go; correct?

25 A. That's what he wrote, yeah.

1           **Q. Do you recall Director Krebs**  
2           **debunking this in a tweet?**

3           A. I suspect, and I keep on, let me  
4           just add, I don't recall Director Krebs'  
5           specific tweet. Two, its possible, as part of  
6           our universe reality page, and Director Krebs  
7           would put a new item up on our universe reality  
8           page, he would tweet out the new universe  
9           reality entry, but I'm not aware of the specific  
10          tweet, but that would be my guess as to what was  
11          going on.

12          **Q. Were you aware that the social**  
13          **media platforms were following the rumor page**  
14          **posted by CISA and using that as a debunking**  
15          **method for content on their platforms?**

16          A. We had a sense they were doing  
17          that, yeah.

18          **Q. And that's kind of the point of it,**  
19          **right, the point of the rumor page is to debunk**  
20          **things; right?**

21          A. No. The point of the page is just  
22          to provide accurate information about rumors  
23          that we were hearing.

24          **Q. Okay. You were aware, I think you**  
25          **just said, that the social media platforms, like**

1       **Twitter, were following the page and using it to**  
2       **fact check, essentially, things that people were**  
3       **posting on their platforms?**

4               A.    Yeah.  So the platforms are looking  
5       for a place to get accurate information about  
6       different things that they were seeing on their  
7       platforms.  And I know some of them used the  
8       universe reality page to do that.

9               **Q.    And, in fact, this e-mail indicates**  
10       **that they used it to debunk the hammer/scorecard**  
11       **narrative, if the tweet that Director Krebs did**  
12       **refers to the rumor page; correct?**

13              A.    I'm sorry, could you repeat the  
14       question?

15              **Q.    Actually, let's move on to the page**  
16       **8625, it's a couple pages down, on page 27 of**  
17       **the PDF.  Here you're flagging, on Friday,**  
18       **November 13th of 2020, you've been flagging a**  
19       **tweet for Twitter.  And at one point you say, at**  
20       **11:26 p.m. on a Friday night, you e-mail Twitter**  
21       **and say:  Some Friday night fun for the two of**  
22       **us, hope you are well; right?**

23              A.    Yeah.

24              **Q.    So you were forwarding and routing**  
25       **disinformation concerns to social media**

1 platforms near midnight on a Friday?

2 A. It appears so.

3 Q. And they were responding in  
4 realtime, for example, 7 minutes later, at 11:33  
5 p.m., Twitter's responding to you late on a  
6 Friday night; correct?

7 A. Yeah.

8 Q. And she says, among other things,  
9 we have labeled so many tweets tonight, so I'm  
10 afraid that the answer is there isn't any  
11 tonight; correct?

12 A. I'm sorry, what are you asking?

13 Q. Directly above, she said: We've  
14 labeled so many tweets tonight that it isn't  
15 ending tonight; correct?

16 A. We have labeled so many tweets  
17 tonight, so I am afraid that for now the answer  
18 is that it isn't ending tonight?

19 Q. Right.

20 A. Yes, that's what she wrote.

21 Q. This is based on an exchange a  
22 little lower down, that you flagged something on  
23 Dominion machines for her, at 11:20 p.m. And  
24 she responded at 11:21 p.m., within one minute,  
25 saying, thanks, Brian, we will escalate;

1 correct?

2 A. Yep, that's what the timestamps  
3 say.

4 Q. Were you getting -- you were kind  
5 of reporting misinformation on social media late  
6 at night to social media platforms during this  
7 timeframe?

8 A. I accidentally closed -- that's page  
9 24?

10 Q. Yeah.

11 A. Sorry. Yeah, as I said, if I were  
12 on my phone, and I saw something come in, I  
13 would push it along.

14 Q. Jump ahead to -- and was it common  
15 for Twitter or Facebook or other platforms to  
16 respond almost immediately, even near midnight  
17 on a Friday?

18 A. I mean, it's hard to say common. I  
19 know it happened. They were generally pretty  
20 responsive. Common's a pretty loose term so,  
21 you know, I don't know how to respond to that.

22 Q. But you say they were generally  
23 responsive, and that includes prompt in their  
24 responses to you?

25 A. Correct. Right. So they were

1 prompt in letting me know that they had received  
2 any e-mail that I sent them, that's essentially  
3 what I was talking about.

4 Q. Let's go to 8557, it's page 42 of  
5 the PDF.

6 A. 42? Okay.

7 Q. Here it looks like Facebook is  
8 e-mailing Lauren Protentis and saying that: I  
9 wanted to share our account security doc that  
10 we've been working on, and we're grateful for  
11 any feedback; right?

12 A. Yep.

13 Q. Do you know what account security  
14 document they're talking about, here in April  
15 15th of 2022?

16 MR. GARDNER: Objection, calls for  
17 speculation.

18 A. Yeah, I don't know what specific  
19 documents they're talking about.

20 Q. Is it possible this is the  
21 one-pager that we were talking about earlier,  
22 does that ring a bell?

23 MR. GARDNER: Objection, calls --  
24 objection, calls for speculation.

25 A. Yeah, I don't -- I don't -- I don't



1 know.

2 Q. Okay. Next page, Lauren Protentis,  
3 thanks so much for sending, this looks great.  
4 The only thing I recommend is any steps for  
5 flagging or escalating MDM content, if possible;  
6 right?

7 A. Yeah, that's what Lauren said.

8 Q. And she said: I think then that  
9 this -- I think, then, that would make this a  
10 comprehensive product on both the critical needs  
11 of officials, account security, and MDM  
12 concerns; correct?

13 A. Yeah, that's what she wrote.

14 Q. She says: We discussed this a bit  
15 in our in-person meeting a few weeks ago; right?

16 A. Yep.

17 Q. Okay. Were you aware of Lauren  
18 asking for Facebook to produce a document and  
19 asking them to include steps for planning or  
20 escalating MDM content for officials?

21 A. I was not aware of this document,  
22 no. I know that the -- I knew those  
23 conversations about the one-pagers we discussed  
24 earlier, but I'm not -- I'm not entirely sure  
25 what this is referring to.

1 Q. Well, I think you said earlier the  
2 one-pagers would talk about what their content  
3 moderation policies are?

4 A. Right.

5 Q. If you look higher, on that same  
6 page, Facebook is replying to Lauren and saying,  
7 would it be -- would it work to just provide my  
8 e-mail when you share out this one-pager; right?  
9 Do you see that?

10 A. So I'm scrolling up.

11 Q. When you share out this one-pager;  
12 do you see that?

13 A. Yes.

14 Q. Okay. So -- so does it seem that  
15 Lauren is talking about the one-pager that all  
16 the social media platforms were asked to provide  
17 for state and local elections; is that what's  
18 going on?

19 A. Again, I'm not sure. It could be  
20 two different one-pagers that she's talking  
21 about, one on account security and one that  
22 Lauren was working on, I wouldn't be -- again, I  
23 wouldn't be surprised if they were similar, but  
24 I -- I can't -- I don't know.

25 Q. Regardless, for the purpose of this

1 one-pager, Lauren is specifically asking that  
2 they add to it a procedure for state officials  
3 to flag and escalate MDM content; correct?

4 A. It appears she's asking for a  
5 process for election officials to report MDM  
6 content to Facebook, yeah.

7 Q. Jump ahead to 12223, here on the --  
8 starting at the 48th page of the PDF and  
9 spilling to the 49th page, there's another  
10 e-mail from Lauren Protentis, this time to  
11 people at Microsoft, which is subject is  
12 one-pager for election officials; do you see  
13 that?

14 A. Did you say 48?

15 Q. Yeah, 48, spilling over onto 49,  
16 it's -- the header's on 48 and the -- oh, I'm  
17 sorry, 43. Bad eyesight. Sorry. It really  
18 looks like an 8.

19 A. That's okay.

20 Q. Sorry, 43.

21 A. I understand that.

22 Okay. So one-pager for election  
23 officials, got the header, okay.

24 Q. And in this e-mail Lauren says to  
25 Microsoft: META is working with industry

1 partners to create one-pagers for election  
2 officials, in the lead-up to the midterms, that  
3 provide steps to create secure accounts --  
4 secure accounts and to report MDM; do you see  
5 that?

6 A. I do.

7 Q. And she said: We'll be sharing  
8 these products at our various engagements with  
9 officials, presumably meaning state and local  
10 election officials; right?

11 MR. GARDNER: Objection, calls for  
12 speculation.

13 A. Yeah, I mean, obviously, I don't  
14 know what she means by officials, but I think  
15 that's a fair assumption.

16 Q. And that's a one-pager for election  
17 officials; correct?

18 A. Yes.

19 Q. Skipping ahead to 22053, page 45 of  
20 the PDF, going onto 46.

21 A. Okay.

22 Q. You see here, on May 11, 2022,  
23 Lauren Protentis is writing to Twitter: Hope  
24 this e-mail finds you well, wanted to circle  
25 back on this and see if you have any questions.

1       **The team has a few upcoming engagements with**  
2       **elections officials for this one-pager, would be**  
3       **particularly helpful to share as a leave behind;**  
4       **correct?**

5               A.    Yes, that's what she's written.

6               Q.    **And Twitter goes back and says:**  
7       **I'll have a one-pager for you later today, just**  
8       **getting the final signoff; right?**

9               A.    Correct.

10              Q.    **And then, once he sends it to him,**  
11       **scrolling back up, first, she says: State and**  
12       **local officials in New Hampshire, Illinois, will**  
13       **be the first recipients of this; right? There**  
14       **at the top of the page.**

15                       **The first line on page 45 of the**  
16       **PDF Lauren says --**

17              A.    Yeah, the e-mail chain is a little  
18       funky, so I was just trying to read and make  
19       sure the e-mails were connected.

20                       Okay. So Twitter provided the  
21       one-pager. Lauren said thanks. State and local  
22       officials in New Hampshire and Illinois will be  
23       the first recipients to this? Okay. Sorry.

24              Q.    **Then she follows up with another**  
25       **e-mail, saying: Actually, one question, is**

1           there a way to include something about how to  
2           report disinformation; do you see that?

3           A.     Yep.    Yep.

4           Q.     And Twitter says:  The best way for  
5           them to do that is to contact gov@twitter.com;  
6           right?

7           A.     Yep.

8           Q.     And I can add that to the doc if  
9           that would be helpful; correct?

10          A.     Correct.

11          Q.     And Lauren says:  That would be so  
12          helpful if you could add that to the doc.  Thank  
13          you; right?

14          A.     Yep.

15          Q.     And Twitter says:  They do; right?

16          A.     Mm-hmm.

17          Q.     So that's the second time she's  
18          pushed the social media platform to expand the  
19          one-pager to include a reporting process for MDM  
20          for the state and local election officials;  
21          correct?

22          A.     I'm not sure that's how I would  
23          characterize it.  I think she's just trying to  
24          make sure that election officials have the  
25          information they need if they want to report.

1 I'm not sure it's expanding. I don't know.  
2 You're making it more dramatic than it was, I  
3 think.

4 Q. Well, suffice to say that she's  
5 asking Twitter to include information  
6 specifically about how do you report MDM;  
7 correct?

8 A. About how election officials should  
9 support MDM, correct.

10 Q. And Twitter had not included that  
11 in theirs, and she asked them to put it in and  
12 they did; right?

13 A. It appears so, yeah.

14 Q. Same thing happened, actually, with  
15 YouTube in your earlier e-mail, right, they  
16 hadn't included it in a one-pager, and she asked  
17 them to put it in; correct?

18 A. I don't recall that e-mail. Which  
19 e-mail is that?

20 (Exhibit No. 27 was marked for  
21 identification.)

22 BY MR. SAUER:

23 Q. Let's move on, actually.  
24 I'm going to e-mail you some new  
25 exhibits.

BRIAN J. SCULLY 1/12/2023

Page 302

1 I'm pulling up Exhibit 27, which  
2 should also be popping up in your inbox.  
3 There's a news report entitled: CISA expands  
4 efforts to fight election disinformation ahead  
5 of challenging 2024 vote; do you see that?

6 MR. GARDNER: Yeah. I'm sorry,  
7 John, we're still waiting for your -- oh, just  
8 got it. Hold on. Hold up. You said 27?

9 MR. SAUER: Yeah.

10 MR. GARDNER: Here you go.

11 THE WITNESS: Okay.

12 BY MR. SAUER:

13 Q. Do you see the headline: CISA  
14 expands efforts to fight election disinformation  
15 ahead of challenging 2024 vote; do you see that?

16 A. I do.

17 Q. What steps are you aware of CISA  
18 taking to expand its efforts to fight election  
19 disinformation going into the next election  
20 cycle, 2024?

21 A. At this time, I'm not aware of any.

22 Q. This is dated August 12th, 2022, if  
23 you scroll down.

24 A. Sure.

25 Q. Were you aware of any discussions



1 or efforts -- any efforts at that time?

2 A. When this was written, in August of  
3 2022? I'm sorry, what time?

4 Q. Well, I'm just saying, are you  
5 aware, around August of 2022, did CISA -- was  
6 CISA expanding efforts to fight disinformation?

7 A. No, no specific efforts, that I'm  
8 aware of, I believe there might have been some  
9 additional funding requested in the budget, but  
10 I'm not sure if that actually went up or not.

11 Q. What -- what efforts did CISA  
12 undertake to fight election disinformation  
13 during the 2022 election cycle?

14 A. We put out a couple of sets of  
15 products.

16 Q. Anything else?

17 A. Not -- not that I recall. We  
18 honestly we didn't do a ton in 2022.

19 Q. What were you guys doing, you're  
20 the MDM team, what did you do to fight MDM?

21 A. So again, our -- as I mentioned,  
22 our role is to build resilience, so we put out  
23 the two sets of products, as I mentioned.  
24 Earlier in 2022, we put out additional products.  
25 I'm sure we gave some stakeholders to build

1 relationships.

2 But generally speaking, we did a  
3 lot of foundational work to better understand  
4 how it functions, those sorts of things, as  
5 opposed to very election-specific activities.

6 Q. Here in the article it says: The  
7 danger -- in the second paragraph -- it says:  
8 The danger of disinformation has become an  
9 incredibly difficult problem, CISA Director Jen  
10 Easterly said on Friday; do you see that?

11 A. I do.

12 Q. And it goes on in his report: That  
13 Easterly has taken several specific steps to  
14 fight the problem, including bringing Kim Wyman,  
15 former Secretary of State of Washington into  
16 CISA to bolster its election work; correct?

17 A. That's what the article says, yep.

18 Q. What has Kim Wyman done to fight  
19 election-related disinformation at CISA?

20 MR. GARDNER: Objection.

21 Objection, lack of foundation, calls for  
22 speculation.

23 BY MR. SAUER:

24 Q. You may answer.

25 A. Yeah, can you be more specific

1 about what you're trying to get to?

2 Q. Well, what does Kim Wyman do at  
3 CISA?

4 A. Kim Wyman is essentially the new  
5 Matt Masterson. So she's a senior advisor to  
6 the director on election security. Most of her  
7 work has been engagement with election  
8 officials. I also think she was CISA's  
9 representative on the CSAC for MDM.

10 So beyond some public speaking  
11 and -- and the CSAC work, I'm not sure what else  
12 she would have done, would have been doing on  
13 MDM.

14 Q. Down here at the very last  
15 paragraph, second page of the document, sorry,  
16 this is hard to highlight, very last paragraph,  
17 it says: While it's not CISA's role to police  
18 social media Easterly said her team has  
19 discussions with platforms, but they're more to  
20 understand large trends, not specific tweets; is  
21 that right?

22 A. That's what the article says, yeah.

23 Q. Do you have discussions with  
24 platforms discussing large trends of online  
25 disinformation?

1           A.    Yeah, I think that's consistent  
2           with what we talked about from the sync meetings  
3           and the discussions around the public reporting  
4           that the platforms have done.

5           **Q.    Any other time when there would**  
6           **be -- where there was discussions with platforms**  
7           **about disinformation trends?**

8           A.    I think it's just the two, the  
9           normal sync meetings we discussed, and then the  
10          normal if they were putting up public reporting  
11          we might get a briefing on it. I'm trying to  
12          think if we ever received -- yeah, I think those  
13          are the big things. We may have done a briefing  
14          where we had a platform maybe talk about -- talk  
15          with election officials, but I'm not sure if I'm  
16          remembering that correctly, so just those two, I  
17          think, would be the main ones.

18                   (Exhibit No. 28 was marked for  
19                   identification.)

20                   MR. SAUER:   Exhibit 28.

21                   MR. GARDNER:   Should be right  
22                   there.

23                   THE WITNESS:   Okay.

24                   BY MR. SAUER:

25                   **Q.    Should be on the screen share, too.**

1                   Here's an e-mail chain, starting  
2                   with Facebook sending an e-mail directly to Jen  
3                   Easterly, saying she had spoken to Facebook  
4                   about receiving a briefing from us on 2022  
5                   election approach; do you see that there, the  
6                   second page of the document, the beginning of  
7                   the chain?

8                   A.     I do.

9                   Q.     Were you aware that Easterly had  
10                  reached out to Facebook directly and asked for,  
11                  I guess in January of 2022, a briefing on how  
12                  Facebook planned to approach the election?

13                  A.     I was not.

14                  Q.     Facebook says: We're happy to do  
15                  this with your team at your convenience, and  
16                  we'd also love to discuss further how we might  
17                  help support the JCDC effort; do you see that?

18                  A.     I do.

19                  Q.     What does JCDC stand for?

20                  A.     I was afraid you were going to ask  
21                  me that. I don't know exactly what it -- what  
22                  it stands for, I think it's joint cyber  
23                  something or another. Sorry, I -- I forget the  
24                  exact acronym, too many acronyms.

25                  Q.     Is it a committee or a subdivision

1       **within CISA or within DHS?**

2               A.    I believe it's a -- it's an effort  
3       by CISA to -- to collaborate with private sector  
4       on cyber defense.

5               **Q.    Okay.  And Director Easterly**  
6       **responds to Facebook saying:  Looping in Kris**  
7       **and teammates to please follow up; do you see**  
8       **that?**

9               A.    I do.

10              **Q.    And then Kris Rose; do you know who**  
11       **Kris Rose is?**

12              A.    My understanding is counselor for  
13       the director, for Director Easterly.

14              **Q.    So -- and he says:  Thank you,**  
15       **Director.  Moving you to BCC; does that stand**  
16       **for blind carbon copy?**

17              A.    That would be my understanding.

18              **Q.    And he says per Geoff, G-e-o-f-f, I**  
19       **presume that's a Geoff Hale; right?**

20              A.    Yeah.

21              **Q.    Sounds like we may want to discuss**  
22       **three primary topics that include 2022**  
23       **elections; right?**

24              A.    Mm-hmm.

25              **Q.    Risk management in the face of**

1       **influence of operations; do you know what that**  
2       **means?**

3               A.    I mean, I don't know what context  
4       he was saying it here, but generally speaking,  
5       that's CISA's mission to reduce risks to  
6       critical infrastructure. So I assume it's risk  
7       management from critical infrastructure to  
8       influence of operations.

9               **Q.    And JCDC, that's the thing you**  
10       **testified before?**

11              A.    Yeah.

12              **Q.    Do you know -- let me ask you this:**  
13       **Were you included in this meeting between**  
14       **Director Easterly and Facebook?**

15              A.    I was not, in fact, I don't know if  
16       the meeting actually ever occurred.

17              **Q.    Do you know if Geoff Hale**  
18       **participated?**

19              A.    I -- I don't.

20                       (Exhibit No. 29 was marked for  
21       identification.)

22       BY MR. SAUER:

23              **Q.    Let's look at Exhibit 29.**

24              A.    Okay.

25              **Q.    Here's a series of text messages**

1 that were produced to us as coming from Director  
2 Easterly.

3 So do you see the blue text, that  
4 would be Director Easterly, the other side, in  
5 the gray, is the interlocutor here on the first  
6 page is this gentleman from Facebook; do you see  
7 that?

8 A. Yeah.

9 Q. This -- he -- he -- he issued a  
10 series of texts. Do you know why he would be  
11 texting Director Easterly, does he know her?

12 MR. GARDNER: Objection, compound.  
13 Objection, calls for speculation.

14 A. Yeah, I -- I don't know is the  
15 short answer. I don't know what their  
16 relationship is.

17 Q. Do you know him, Mr. Gleicher?

18 A. Yeah, I know Nathaniel Gleicher,  
19 yeah.

20 Q. Does he interact with CISA about  
21 misinformation issues on Facebook?

22 A. He does, he participates in the  
23 monthly regular meetings that we talked about.

24 Q. What else does he do, do you know,  
25 for Facebook on --



1 A. I'm sorry, what was the last part?

2 Q. What else does he do for Facebook  
3 on misinformation?

4 A. Again, I think he would articulate  
5 the inoffensive behavior, coordinating  
6 inoffensive behavior. So I don't know if he  
7 would talk about it in the context of  
8 disinformation. But my understanding is he  
9 leads the team one of the teams that deals with  
10 the coordinated inoffensive behavior.

11 Q. Let me ask you about Rob Silvers.  
12 Do you know who Rob Silvers?

13 A. Yes.

14 Q. Who's Rob Silvers?

15 A. He heads up the DHS office of  
16 policy. I don't know what his back title is,  
17 assistant secretary or secretary, something like  
18 that.

19 Q. So he's in the secretary's office?

20 A. I believe he reports up to the  
21 secretary, yeah.

22 Q. He -- he -- and Mr. Gleicher says  
23 to Jen Easterly: Do you have any context you  
24 can share in the role Rob Silvers is playing on  
25 disinfo; right?

1 A. Yep, that's what the text says.

2 Q. I understand his team is a task  
3 force set up, and it was suggested that his team  
4 is handing policy on disinfo while CISA is  
5 handling operations; right?

6 A. Yeah, that's what Nathaniel wrote.

7 Q. What is -- what was your  
8 understanding of Rob Silver being involved in  
9 policy on disinformation?

10 A. So that is the DHS office of  
11 policy. He would be involved in most, I would  
12 say, policy activities related to any topic that  
13 crossed the department, including  
14 disinformation.

15 Q. And Director Easterly says she's  
16 happy to chat with Mr. Gleicher; right?

17 A. Yep.

18 Q. You don't know if they actually  
19 talked to each other, do you?

20 A. I don't.

21 Q. She goes on to say: Rob is running  
22 a governance board to look at potential new  
23 areas of confronting MDM; correct?

24 A. That's what she wrote, yeah.

25 Q. Then she says: It doesn't change

1 or impact anything, we, meaning CISA, are doing  
2 or have already established; right?

3 A. Yes, that's what she wrote.

4 Q. What were the potential -- what  
5 potential new areas of confronting MDM were  
6 discussed, do you know?

7 MR. GARDNER: Objection, lack of  
8 foundation.

9 A. I don't have any clue.

10 Q. Next page, there's an e-mail from  
11 Matt Masterson to the director; right?

12 A. Yep.

13 Q. This is a -- Matt Masterson know  
14 the director well, I take it he was a political  
15 appointee, did you say that?

16 A. In previous administration --  
17 excuse me -- yeah, he was a political appointee.  
18 I don't know what his relationship with the  
19 director was, so I don't know how well he knew  
20 her.

21 Q. What was the director's role in the  
22 previous administration, was she at CISA?

23 A. No. Director Easterly was not at  
24 CISA, no.

25 Q. Who was she?

1 A. I'm sorry?

2 Q. Was she in government?

3 A. Prior to the -- in the previous  
4 administration?

5 Q. Yeah.

6 A. I don't know. I think her  
7 immediate previous job was in the private  
8 sector, but I don't know how long and if she  
9 spent any time, at all, in the -- in the  
10 previous administration in government.

11 Q. And here, Director Easterly says to  
12 Matt Masterson, just trying to get us in a place  
13 where FED can work with platforms to better  
14 understand the mis, dis trends so relevant  
15 agencies can try to prebunk/debunk as useful;  
16 correct?

17 A. That's what she wrote, yeah.

18 Q. And that discussion of trends is  
19 similar to her statement in the media article we  
20 just looked at about how CISA is interacting  
21 with social media platforms to identify trends;  
22 correct?

23 A. She mentioned trends in both,  
24 correct.

25 Q. And here she -- the reason she

1       wants to understand the trends from the  
2       platforms is so that the relevant agencies can  
3       try to prebunk or debunk the mis and  
4       disinformation; correct?

5               A.    Yeah, I think that's what she's  
6       saying.

7               Q.    Can you do that at CISA, when you  
8       find out about a trend do you go try to work  
9       with another federal agency to prebunk or debunk  
10      it?

11              A.    So again, from a resilience-  
12      building perspective, you know, what we try to  
13      do is provide accurate information about those  
14      issues and topics that are relevant to us. So  
15      from an election perspective we would try to  
16      provide appropriate information about elections,  
17      so that the universe reality page would be an  
18      example of that, it would fall more potentially  
19      into the debunking side.

20              Prebunking is trying to understand  
21      ahead of time what could happen so you could  
22      fill information gaps.

23              And so that's generally kind of how  
24      resilience works. So yeah, we would -- we would  
25      try to do some of that.

1 I don't know -- so we worked a  
2 little bit with the FBI, on products or  
3 resilience-based products, as I mentioned. I  
4 say that's probably -- we worked, as I mentioned  
5 earlier, we worked with the GAC initiative about  
6 tactics and such.

7 So those are the types of things  
8 that we would do to, again, help people  
9 understand how MDM works and steps they can take  
10 to reduce the risks.

11 **Q. Her next text here, Director**  
12 **Easterly's next text says: Not our mission, but**  
13 **was looking to play a coord role so not every**  
14 **D/A is independently reaching out to platforms**  
15 **which could cause a lot of chaos; right?**

16 A. That's what she wrote, yep.

17 **Q. What does D/A mean, is that**  
18 **department or agency?**

19 MR. GARDNER: Objection, calls for  
20 speculation.

21 BY MR. SAUER:

22 **Q. If you know.**

23 A. That's -- that is one of our common  
24 abbreviations for department and agency, but I'm  
25 not sure if that's what she's referring to here.

1 Q. Do you know -- let me ask this: Do  
2 you believe that if every federal department and  
3 agency is independently reaching out to the  
4 platforms that could cause chaos?

5 A. Yeah, I think chaos might be a  
6 little strong. But, you know, it does create  
7 challenges and provides the platforms  
8 opportunities to play departments off each  
9 other.

10 Q. Does -- does CISA try to play a  
11 coordinating role in that, in other words,  
12 coordinating between the federal agencies and  
13 the social media platforms on disinformation and  
14 misinformation issues?

15 A. So we did do that as it relates to  
16 the sync meetings we discussed throughout the  
17 testimony. Beyond that, we didn't -- we didn't  
18 attempt to play a substantial role in terms of  
19 coordinating between.

20 Q. Let me ask you this: Matt  
21 Masterson responds to this e-mail or this text  
22 and says: We'll get there, and that kind of  
23 leadership really helps. Platforms have got to  
24 get more comfortable with government. It's  
25 really interesting how hesitant they remain;

1 correct?

2 A. That's something I wrote.

3 Q. Is that consistent with your  
4 experience that the social media platforms have  
5 to be kind of pushed or encouraged to coordinate  
6 with the government on misinformation issues?

7 A. I don't think that's how I would  
8 characterize it. You know, we operate in a  
9 voluntary kind of manner, so it's voluntary  
10 whether -- for CISA, again, for CISA, the MDM  
11 team, so it's always up to the platforms what  
12 level of engagement they want to have with us.

13 Q. Do you know whether Masterson and  
14 Easterly had any further discussion of these  
15 issues?

16 A. I don't know.

17 Q. Let me send you a couple more  
18 exhibits. And while they are coming, do you  
19 know, were you involved, at all, in the  
20 formation --

21 MR. GARDNER: I'm sorry, John, I'm  
22 sorry, the witness just asked me if we can take  
23 a break.

24 MR. SAUER: Oh.

25 THE WITNESS: Just a few minutes,



1 bathroom break.

2 MR. SAUER: Well, why don't we make  
3 it five, and try to make it the last break of  
4 the day. How long have we been on the record?

5 MR. SCOTT: We got back on at 3:50,  
6 so it's 4:40, so it's 50 minutes in, we have an  
7 hour and 10 minutes left.

8 MR. GARDNER: He's been reliable.  
9 We need to do this off the record, first of all.

10 THE VIDEOGRAPHER: The time is now  
11 4:42. We are off the record.

12 (Recess.)

13 THE VIDEOGRAPHER: The time is  
14 4:53. We are back on the record.

15 (Exhibit No. 30 was marked for  
16 identification.)

17 BY MR. SAUER:

18 Q. Exhibit 30 should be in your inbox.  
19 I'll put it up on the screen share.

20 Here's an article in The Intercept  
21 called Truth Cops, Leaked Documents Outline  
22 DHSA's Plans to Police Disinformation; do you  
23 see that?

24 A. Yeah, we don't have it on here, but  
25 I saw the headline in your screen share.

1 Q. Okay. Sorry. But scrolling down,  
2 still on the first page, it says: The  
3 Department of Homeland Security is quietly  
4 broadening its effort to curb speech it  
5 considers dangerous; do you see that?

6 A. I see that in the article, yep.

7 Q. Are you aware of DHS broadening its  
8 efforts to address disinformation?

9 A. I am not, no.

10 Q. Has CISA been expanding its MDM  
11 team?

12 A. As I mentioned earlier, we have  
13 not.

14 Q. Let me ask you this: Scrolling  
15 down here, third page of the document, it says:  
16 There is also a formalized process for  
17 government officials to directly flag content on  
18 Facebook or Instagram and request that it be  
19 throttled or suppressed through a special  
20 Facebook portal that requires a government or  
21 law enforcement e-mail to use; do you see that?

22 A. Yeah, I see that in the article.

23 Q. And it actually provides a link for  
24 it, [Facebook.com/Xtakedowns/login](https://www.facebook.com/Xtakedowns/login); are you aware  
25 of that reporting channel for government

1 officials?

2 A. I am not, no.

3 Q. On the next page, fourth page of  
4 the document, it says: According to a draft  
5 copy of DHS's quadrennial Homeland Security  
6 review, DHS's capstone report outlining the  
7 department's strategy and priorities in the  
8 coming years, the department plans to target  
9 inaccurate information on a wide range of  
10 topics; do you see that?

11 A. Yeah, I see that in the article.

12 Q. Are you aware of the document  
13 that's a draft of the quadrennial Homeland  
14 Security review?

15 A. I know it says quadrennial Homeland  
16 Security review is, I don't know if I've seen  
17 the draft of the most recent one.

18 Q. Have you seen any drafts of the  
19 most recent one?

20 A. Not that I recall.

21 Q. When does it -- when does it get  
22 finalized?

23 A. I -- I -- I don't know.

24 Q. It says: Including the origins of  
25 the COVID-19 pandemic and the efforts of the

1 COVID-19 vaccines, racial justice, US withdrawal  
2 from Afghanistan, and the nature of US support  
3 for Ukraine, in quotes; do you see that?

4 A. I do.

5 Q. Are you aware of discussions  
6 anywhere in DHS about addressing misinformation  
7 about the origins of the COVID-19 pandemic?

8 A. I am not.

9 Q. So how about the efficacy of  
10 COVID-19 vaccines?

11 A. Yes, I'm aware of some discussions  
12 on that.

13 Q. What discussions are you aware of?

14 A. So it was a -- as I mentioned  
15 earlier, our building critical infrastructure  
16 help in public health is one of the sectors of  
17 critical infrastructure, so we engage with CDC  
18 and HHS to help them. We've also put out one  
19 product, sometime in mid 2020, for  
20 infrastructure stakeholders about COVID-related  
21 disinformation.

22 Q. What do you do to assist CDC and  
23 HSH?

24 A. For the most part, not a lot, to be  
25 honest. Like I said, we did the one product

1 related to them, and we just participate in  
2 meetings with them. From our perspective,  
3 again, we're trying to understand trends, how  
4 this information is spreading tactics so we can  
5 help the public, the public and organizations,  
6 critical infrastructure organizations, as well  
7 as some others, understand the risks from MDM  
8 and how it works and what they can do about it.

9 **Q. Do you -- do you obtain information**  
10 **from CDC and HHS about how COVID vaccine**  
11 **misinformation spreads?**

12 A. I believe that they provided some  
13 briefings on that, yeah.

14 **Q. And do you also provide briefings**  
15 **to them or information to them?**

16 A. We did some work on the kind of  
17 bio-lab narratives, so this is essentially  
18 foreign governments, whenever anything happens,  
19 whether biological and sometimes not, they will  
20 point to US biolabs as being the culprit behind  
21 it, and so as part of our resilience-building  
22 efforts we're trying to understand how foreign  
23 actors have used that narrative over time.

24 And so we, starting back in the  
25 '80s, probably since back in the '80s, the

1 Russians were using that. Usually they're  
2 saying at Fort Detrick or some other kind of US  
3 entity is a biolab, and that's where whatever it  
4 starts.

5 We saw this with COVID. We saw  
6 this Monkey Pox. We saw this around Ukraine.  
7 And so, again, just helping people understand  
8 that a lot of these disinformation narratives  
9 are recycled over time, for different issues, as  
10 a way to help build resilience.

11 **Q. How about racial justice, are you**  
12 **doing anything to address misinformation about**  
13 **racial justice issue?**

14 A. CISA has not, to my knowledge, done  
15 anything related to racial justice.

16 **Q. How about other DHS components, do**  
17 **they do anything on that?**

18 A. Not that I'm aware of, but  
19 obviously I don't know everything that they do.

20 **Q. How about US withdrawal from**  
21 **Afghanistan, does CISA work on that?**

22 A. Not that I'm aware of.

23 **Q. And how about other DHS components?**

24 MR. GARDNER: Objection, calls for  
25 speculation.

1 A. Yeah, I -- I'm not aware of what  
2 other components are doing.

3 Q. And then the nature of US support  
4 to Ukraine?

5 A. So there was a department stood  
6 out, what's called the Unified Coordination  
7 Group, when Russia invaded Ukraine, to  
8 coordinate DHS activities related to the crisis.  
9 As a part of that there was an MDM component,  
10 and a member of the MDM team was detailed to  
11 lead the MDM component of the Russian/Ukraine  
12 work. I believe it lasted about two months.

13 Q. What did they do?

14 A. The Unified Coordination Group.  
15 Sorry.

16 Q. What did that group do?

17 A. So most of it took place while I  
18 was out, so I don't have a super clear  
19 understanding of everything, but generally  
20 speaking, they provided a -- they would monitor  
21 open source researching.

22 So we talk about third-party  
23 researchers, we put out reports, and things like  
24 that, and they would provide situational  
25 awareness, at least from our perspective, CISA

1 perspective, they would provide situational  
2 awareness up to the MDM Unified Coordination  
3 Group.

4 **Q. Who at CISA participated in that?**

5 A. So Rob Schaul from the MDM team was  
6 detailed to the Unified Coordination Group, and  
7 then several members of the team would have been  
8 monitoring open source.

9 So we have the open source  
10 reporting. These are third-party research  
11 reports, things like that, to point to  
12 information to just make leadership aware.

13 **Q. Did they -- did that group  
14 communicate with social media platforms about  
15 disinformation relating to Ukraine?**

16 A. By that group, do you mean Unified  
17 Coordination Group?

18 **Q. Correct.**

19 A. I -- I don't know.

20 **Q. Rob Schaul would know that?**

21 A. He led the team, so I suspect he  
22 might.

23 **Q. Do you know if that team  
24 communicated with social media platforms, at  
25 all?**



1           A.    I don't know.  There was a call, at  
2           some point, early, between -- between critical  
3           infrastructure and I believe some social media  
4           around that, but I wasn't around for that call  
5           so I don't really know the nature of what was  
6           discussed or anything along those lines.

7           **Q.    There was a call between -- and I'm**  
8           **sorry, I couldn't hear clearly what you said --**  
9           **there was a call between social media platforms**  
10          **and -- and who?**

11          A.    So I believe the way I understand  
12          the call is it facilitated a call with critical  
13          infrastructure, the critical infrastructure  
14          community, to private sector companies, sector  
15          risk management agencies, folks that were  
16          involved in critical infrastructure security.  I  
17          believe, my understanding is that call did  
18          include some social media platforms.

19          **Q.    And you -- but you don't know what**  
20          **was said in that call?**

21          A.    No, I wasn't -- I wasn't back at  
22          CISA yet.

23          **Q.    Do you know when the call occurred?**

24          A.    It would have been in probably the  
25          February -- February time -- timeframe, I would

1 think.

2 Q. February 2022?

3 A. Correct.

4 (Exhibit No. 31 was marked for  
5 identification.)

6 BY MR. SAUER:

7 Q. I'm putting up Exhibit 31 on the  
8 screen share. You should have it in front of  
9 you.

10 A. Okay. I got it.

11 Q. Here's a report from the Office of  
12 the Inspector General, entitled: DHS needs a  
13 unified strategy to counter disinformation  
14 campaigns; do you see that?

15 A. I do.

16 Q. Are you familiar with this OIG  
17 report?

18 A. Mostly familiar with it, yeah.

19 Q. Were you aware that they -- do you  
20 know what the day of the report is?

21 A. Says August 10th, 2022.

22 Q. And I take it this report is  
23 recommending that here to what we have found,  
24 DHS needs unified strategy or -- to address  
25 disinformation; right? Right here, it says:

1 DHS does not yet have a unified department-wide  
2 strategy to effectively counter disinformation  
3 that originates from both foreign and domestic  
4 sources; correct?

5 A. I'm trying to find that. Okay.

6 Q. Yeah.

7 A. DHS does not yet have a unified  
8 strategy. Correct, yeah, that's what's written  
9 there.

10 Q. Do you share that view, do you  
11 think DHS lacks a department-wide strategy?

12 A. Yes.

13 Q. Do you think that different  
14 components of DHS are engaging in different sort  
15 of MDM-related activities without coordinating  
16 with each other?

17 A. Yeah, I think that's a fair  
18 assumption.

19 Q. Were you aware that this  
20 recommendation was made for DHS to do internal  
21 and external coordination better?

22 A. Was I aware that this report was  
23 stating that DHS needs to do better in internal  
24 and external coordination?

25 Q. Yeah.

1 A. I -- I don't know if that's what it  
2 says, is there a page in here where that  
3 recommendation is or those recommendations?

4 Q. Let's go to page 7.

5 A. Is this PDF 7 or document page 7?

6 Q. Good question. It's PDF 9,  
7 document --

8 A. PDF 9? Okay.

9 Q. It's here underneath the graphic  
10 novels images, there's a paragraph that begins:  
11 More recently; do you see that?

12 A. Yep.

13 Q. It says: In January 2021 CISA  
14 transitioned its countering foreign influence  
15 task force to promote more flexibility to focus  
16 on general MDM; right?

17 A. Mm-hmm, that's what it says.

18 Q. And that CISA's got 15 dedicated  
19 part- and full-time staff; is that still true?

20 A. No.

21 Q. I'm sorry, the MDM team has 15  
22 staff; is that still true?

23 A. No.

24 Q. How many does it have?

25 A. Right now, we have five full-time

1 staff plus one on maternity leave, so six. And  
2 then we have one, two, two contractor's  
3 support -- no, three contractor's supporting us.

4 **Q. Did at some time you have 15 people**  
5 **working on this on the MDM team?**

6 A. I suspect at the height of the team  
7 if you add in all the contractors there it  
8 probably got close to 15, but I'm not sure of  
9 the exact number.

10 **Q. When was the height of the team?**

11 A. Staff plus contractors was  
12 probably -- good question. When was the height  
13 of the team? We didn't have much contract  
14 support in 2020, so I would probably say 2021,  
15 while I was gone.

16 **Q. It says: The MDM team focuses on**  
17 **disinformation activities targeting elections**  
18 **and critical infrastructure. According to a**  
19 **CISA official, the MDM team counters all types**  
20 **of disinformation, to be responsive to current**  
21 **events; is that right?**

22 A. That's what the document says, yep.

23 **Q. Is that true that the MDM team**  
24 **counters all types of disinformation to be**  
25 **responsive to current events?**

1           A.    We, again, try to build resilience  
2           and reduce risks to critical infrastructure.  So  
3           I -- you know, if the event could impact  
4           critical infrastructure, that would be something  
5           we would consider addressing.

6           **Q.    Does critical infrastructure**  
7           **include cognitive infrastructure?**

8           A.    Not through national policy.

9           **Q.    Okay.  Let me go two pages further,**  
10          **paragraph -- page 9, it says:  For example,**  
11          **according to an ODNI official, prior to the**  
12          **November 2020 elections CISA and I&A joined in**  
13          **weekly teleconferences to coordinate**  
14          **intelligence community activities to counter**  
15          **election-related disinformation; correct?**

16          A.    That's what the document says, yes.

17          **Q.    Were you aware of those calls,**  
18          **that's a coordinating call between CISA, I&A and**  
19          **ODNI?**

20          A.    No, that was a coordinate -- so  
21          yeah, from the call, but the calls were DNI-led  
22          coordination calls of the intelligence  
23          community.  CISA was there mostly from an  
24          observer standpoint, to do as an election  
25          security lead.  But it was -- it was an intel

1 community-focused coordination and conversation.

2 Q. Who from CISA participated in those  
3 calls?

4 A. I think it was just a random -- a  
5 random mix. Geoff did not generally participate  
6 in them. I didn't generally participate in  
7 them, although I think I did maybe once or  
8 twice, normally somebody at the staff level.

9 Yeah, we have an intel office in  
10 CISA, so I suspect that at least somebody from  
11 the intel office was on the calls. But I think  
12 it was just, you know, it was who's available at  
13 the staff level would go participate at that  
14 time.

15 Q. Was disinformation, you know, how  
16 to combat disinformation on social media, is  
17 that discussed in these calls?

18 MR. GARDNER: Objection, calls for  
19 speculation, lack of foundation.

20 A. My understanding, my recollection  
21 of the calls, at least the couple I was on, it  
22 was generally the intel community talking about  
23 what products they were developing, what  
24 analysis they were doing, things along those  
25 lines.

1 Q. The next sentence says: The office  
2 of the DNI official stated the teleconferences  
3 continue to occur every two weeks after the 2020  
4 elections, and were still taking place at the  
5 time of this audit in August of 2022; do you see  
6 that?

7 A. I do.

8 Q. Yeah, what -- are those calls still  
9 going on today, every two weeks?

10 A. I don't know. That was -- that's  
11 a -- THAT they're still continuing to November  
12 of 2022 is news to me. So yeah, I don't -- as  
13 far as I know, we weren't participating in them.  
14 I wouldn't be surprised if there was some calls  
15 going on, but I don't recall. The intel  
16 community doesn't tell community things when I  
17 was involved in that.

18 Q. Why don't I e-mail you another  
19 exhibit, 27.

20 MR. GARDNER: John, if you just  
21 spoke, I couldn't hear you, but sound wasn't  
22 coming through.

23 MR. SAUER: I'm sorry. Yeah,  
24 actually, I'm going to skip that one. I meant  
25 Exhibit 23, which I'm now e-mailing you.



1 MR. GARDNER: Not Exhibit 27?

2 MR. SAUER: 27 should look familiar  
3 to you. We talked about it already.

4 MR. GARDNER: Okay. Just to be  
5 clear, are we talking about 27 now or a  
6 different exhibit?

7 MR. SAUER: 23.

8 MR. GARDNER: Okay. Don't have  
9 that yet, but as soon as we do.

10 MR. SAUER: And I'm putting it up  
11 on the screen share, too.

12 (Exhibit No. 23 was marked for  
13 identification.)

14 BY MR. SAUER:

15 Q. Here's a November 2021 report on  
16 public comments by Director Easterly and The  
17 Hill; do you see that?

18 A. Yes.

19 Q. It says: The title is cyber agency  
20 beefing up disinformation misinformation team;  
21 correct?

22 A. Correct.

23 Q. And in the first paragraph says:  
24 CISA is beefing up its disinformation and  
25 misinformation team in the wake of a dismissive

1       **precedential election that saw a proliferation**  
2       **of misleading online information; correct?**

3             A.    Yeah, that's what the article says.

4             **Q.    Were you aware of efforts to beef**  
5       **up the misinformation team in November of '21?**

6             A.    No, not specific efforts. I was  
7       over at the National Security Council at the  
8       time.

9             **Q.    When did you come back from that**  
10       **detail?**

11            A.    The detail officially ended in  
12       early March, and I took some leave and started  
13       back at CISA in early to mid April.

14            **Q.    And the director says in the next**  
15       **paragraph: I'm actually going to grow and**  
16       **strengthen my misinformation and disinformation**  
17       **team; do you see that?**

18            A.    I do.

19            **Q.    I know you were on detail then, are**  
20       **you aware of efforts to grow and strengthen the**  
21       **team, for example, by adding new people?**

22            A.    Again as I mentioned earlier in my  
23       testimony, my understanding is there was some  
24       budget increase that was proposed. I don't -- I  
25       don't know if that moved forward or not, from

1 the department.

2 Q. Is the -- do these remarks coincide  
3 with what you said was kind of the high point,  
4 when you had 15 people on the MDM team, was that  
5 around, you know, November 2021?

6 A. It's hard to say for sure. I'm  
7 not -- I'm not sure how they're counting  
8 positions. So I don't think we ever had 15  
9 federal employees. So there's, you know, it  
10 seems to me like they were probably counting  
11 contract support, so -- so it's hard for me to  
12 say exactly when that would have been.

13 Q. You say there was, in this  
14 timeframe, some attempt to get budget authority  
15 to add people to the MDM team?

16 A. It was my understanding that there  
17 was a request for additional funds made to the  
18 budget. But again, I don't know, the budget  
19 process is a little bit of a mystery to me, so  
20 I'm not sure what exactly happened along the  
21 way, if it ended up in the -- you know, in the  
22 budget requests or what.

23 Q. The next paragraph says that  
24 Easterly noted that earlier this week she had a  
25 meeting with six of the nation's experts in that

1           **misinformation and disinformation space; do you**  
2           **see that?**

3           A.     I do.

4           **Q.     Do you know who she met with?**

5           A.     I don't.

6           **Q.     Do you know who are six of the**  
7           **nation's experts in disinformation and**  
8           **misinformation?**

9           A.     I mean, I could come up with a list  
10          of experts. I don't know if that's who she met  
11          with.

12          **Q.     She stressed her concerns around**  
13          **this being a top threat for CISA; correct?**

14          A.     That's what the article says, yep.

15          **Q.     And it goes on to quote her,**  
16          **saying: One could argue we're in the business**  
17          **of critical infrastructure, and the most**  
18          **critical infrastructure is our cognitive**  
19          **infrastructure; correct?**

20          A.     That's what the quote says, yep.

21          **Q.     Do you -- do you -- do you -- does**  
22          **the MDM team view protecting our cognitive**  
23          **infrastructure as part of its mission?**

24          A.     No. We look at the -- again, the  
25          international policy there's, like, 16 sectors,

1 and those are the critical infrastructure  
2 factors we look to protect. So we wouldn't  
3 include cognitive infrastructure in that list.

4 **Q. One of them is election**  
5 **infrastructure; is that right?**

6 A. Election infrastructure is actually  
7 a subsector of the government's stability  
8 structure.

9 **Q. So if someone posts information on**  
10 **social media implying that, you know, ballots**  
11 **were being shredded by poll workers, what**  
12 **infrastructure is that a threat to?**

13 MR. GARDNER: Objection, calls for  
14 a hypothetical.

15 A. Yeah, I would rather not answer  
16 hypotheticals.

17 **Q. You have no instruction not to**  
18 **answer, please answer the question.**

19 MR. GARDNER: Same objection.

20 A. Yeah, I'm not answering a  
21 hypothetical.

22 **Q. Please answer the questions. If**  
23 **someone posts on social media --**

24 A. Can you give me an example of the  
25 post?

1 Q. If you look at all the posts we  
2 looked at earlier in your e-mails, where, for  
3 example, suppose someone posts the hammer and  
4 scorecard conspiracy on social media, and  
5 Director Krebs tells you to reach out to social  
6 media platforms to see what they're doing about  
7 it, how does the posting about the hammer and  
8 scorecard narrative on social media threaten  
9 critical infrastructure?

10 A. So it -- so generally speaking,  
11 this mis, mal-information threatens critical  
12 infrastructure in a number of ways, it could be  
13 operational impact, so in the case of the  
14 elections, disrupting election operations,  
15 things along those lines. It could be human  
16 impact, so again, see election example, there's  
17 a lot of threats of violence made against  
18 election officials, making it harder to do their  
19 jobs.

20 So a multitude of ways that  
21 disinformation could impact critical  
22 infrastructure, like I said, we -- you know,  
23 there's financial, there's reputational, there's  
24 just a multitude of ways that this  
25 disinformation could affect critical

1 infrastructure.

2 **Q. Does infrastructure have a**  
3 **reputational interest?**

4 A. Does infrastructure have a  
5 reputational interest?

6 MR. GARDNER: Objection, vague.

7 THE WITNESS: Yeah, could you be a  
8 little more specific.

9 BY MR. SAUER:

10 **Q. You just used the word, you said**  
11 **there's financial, there's reputational, what do**  
12 **you mean by that? What is the reputational**  
13 **threat to critical infrastructure from social**  
14 **media postings?**

15 A. Well, I wouldn't -- I wasn't saying  
16 specifically from social media postings. I was  
17 saying from fraud, from mis, dis and  
18 mal-information, a reputational risk could come  
19 about if the integrity or the public confidence  
20 in a particular sector was critical to that  
21 sector's functioning.

22 So I think the financial services  
23 would probably be a good example. So if there's  
24 a loss of confidence by the American public in  
25 financial services, financial systems of the

1 United States, that could create national  
2 security concerns.

3 **Q. Explain that to me, how would a**  
4 **loss of confidence in the financial system**  
5 **create national security concerns?**

6 A. Lots of ways, you can have runs on  
7 banks, such as the banking, you could have, you  
8 know, other sorts of issues related to that, so  
9 yeah, so there's -- you know, if there's a loss  
10 of confidence, if there's a run on banks and  
11 there's a run on the financial systems, those  
12 sorts of things can create physical harms,  
13 operational harms.

14 So again, if we go back to the list  
15 of potential harms, the reputational could lead  
16 to operational, right? So banks could be  
17 overwhelmed with people showing up trying to  
18 take money out. They could be overwhelmed with  
19 people showing up elsewhere at other facilities  
20 and disrupt our operations. So it's a full  
21 range of potential risks. A lot of these are  
22 cascading, and so, yeah.

23 **Q. So is it part of the MDM team's job**  
24 **and CISA's job to counter disinformation that**  
25 **creates reputational risks to, for example, the**



1 **financial services industry?**

2 A. So again, our mission is to build  
3 resilience. And so we would work -- if the  
4 financial services sector wanted us to work with  
5 them, to develop products to help them  
6 understand how mis, dis and mal-information  
7 could impact their -- their sector, we would --  
8 we would work with them on that yes.

9 **Q. What sorts of mis, dis and**  
10 **mal-information might undermine confidence in**  
11 **the financial services?**

12 A. I don't know. We haven't -- we  
13 haven't dealt with that. We're not financial  
14 services experts, so we generally defer to a  
15 department or agency.

16 So in this case, Treasury, the  
17 sector risk management agency responsible for  
18 the financial services sector, so our expertise  
19 with the MDM team is understanding MDM and  
20 potentially to mitigate risks and to build  
21 resilience, and so we wouldn't be the experts on  
22 the actual financial services MDM.

23 **Q. So everything you just said about**  
24 **the financial services was a lengthy**  
25 **hypothetical?**

1           A.    Like I said, I don't like getting  
2           into hypotheticals.

3           **Q.    You did for awhile, there.**

4                       **Scrolling down in the same**  
5           **document, it says -- there's a quote from**  
6           **Director Easterly, where she says now --**

7                       MR. GARDNER:  Sorry, hold on.

8                       MR. SAUER:  Can you guys hear me  
9           now?

10                      MR. GARDNER:  Yeah.

11                      MR. SAUER:  Okay.

12  BY MR. SAUER:

13                      **Q.    Quote from Director Easterly, we**  
14           **now live in a world where people talk about**  
15           **alternative facts, post truth, which I think is**  
16           **really, really dangerous, if you get to pick**  
17           **your own facts, and it's particularly corrosive**  
18           **when you talk about matters of election**  
19           **security; right?**

20                      A.    That's the quote, yeah.

21                      **Q.    And is that kind of consistent with**  
22           **what the MDM team does, it tries to prevent a**  
23           **situation where Americans get to pick their own**  
24           **facts?**

25                      MR. GARDNER:  Objection, vague.

1           A.    I -- I -- that's -- no, that's not  
2 consistent with what we do.

3           **Q.    So that's -- that's not a -- you**  
4 **don't think Director Easterly's description is**  
5 **very fair?**

6           MR. GARDNER:  Objection,  
7 mischaracterizes the witness's previous  
8 testimony.

9           A.    Yeah, if I understand your question  
10 you said that CISA played a role in alternate  
11 facts and post truths and things like that, and  
12 CISA does not do that sort of thing.

13           MR. SAUER:  Sending you a few more  
14 exhibits by e-mail.  You should be getting two  
15 e-mails, the first one with three attachments,  
16 and the second one with one.

17                    It may take a minute.  It's loading  
18 slowly on my end.  Okay.  I'm opening Exhibit  
19 49, and I'll put that on the screen share.

20                           (Exhibit No. 49 was marked for  
21 identification.)

22 BY MR. SAUER:

23           **Q.    Did you give an interview to the**  
24 **Berkman Klein Center on June 18th of 2020?**

25           A.    I don't recall the specific date,

1 but I did give them an interview, so that's  
2 probably about right.

3 Q. And this is an interview by The  
4 Breakdown. And do you recall doing this  
5 interview?

6 A. I do.

7 Q. On the third page of the document,  
8 you say: For us, in particular -- oops, it  
9 didn't highlight well -- for us, in particular,  
10 you see here, it's the second bullet -- for us,  
11 in particular, we're trying to reduce the amount  
12 that Americans engage with disinformation;  
13 right?

14 A. Yes.

15 Q. Is that -- to your mind, is that a  
16 good summary of what the MDM team does, it tries  
17 to reduce the amount that Americans engage with  
18 disinformation?

19 A. That's the general idea behind  
20 resilience-building, yeah.

21 Q. What is engaging with  
22 disinformation?

23 A. Amplifying it, re-tweeting it,  
24 resending it, things like that.

25 Q. How about liking it on social

1 media, is that a form of engagement?

2 A. Yep.

3 Q. How about just reading it, is that  
4 a form of engagement?

5 A. No.

6 Q. So if you're reading disinformation  
7 is not engagement with it?

8 A. Correct.

9 Q. But -- but so engagement is taking  
10 some affirmative step further, like you said,  
11 amplify, like, repost, that's kind of  
12 disinformation, in your view, I'm sorry, that's  
13 engagement; correct?

14 A. Yes.

15 Q. And it's part of CISA's or the --  
16 CISA's job to try to reduce the amount that that  
17 happens; right?

18 A. I wouldn't characterize it that  
19 way. I would say the ultimate goal of building  
20 resilience is that people are less likely to  
21 amplify mis and disinformation.

22 Q. And that's what you're trying to do  
23 at the MDM team, is reduce the amount that  
24 Americans engage with disinformation?

25 A. Yeah, through public awareness and

1 public engagement and things like that, yep.

2 Q. The last page of the document, you  
3 say -- here there's a paragraph where you say:  
4 The question is, we have people calling for more  
5 monitoring of speech on platforms. And then you  
6 go on to say: We have to built the platforms  
7 that this is a lie and they need to take it down  
8 or we're asking the platforms to do that; right?

9 A. Yeah, that's what -- that's what  
10 the quote is, yep.

11 Q. Okay. Is that, in fact, what the  
12 MDM team is doing or I guess it was countering  
13 foreign influence task force team was doing in  
14 2020 when it was routing disinformation concerns  
15 to Facebook, were you telling them to --

16 A. No.

17 Q. Go ahead.

18 A. No. Essentially what this quote is  
19 saying is that in the general conversation about  
20 how to address mis and disinformation there are  
21 a lot of people saying that we should -- the  
22 government should be the ones taking things  
23 down, or the government should be asking the  
24 platforms to do certain things, and that's not  
25 necessarily the right spot for government to be.

1           Q.    So when you say: We have to tell  
2   the platforms that this is a lie and they need  
3   to take it down, you're attributing that view to  
4   other people, not yourself?

5           A.    Yeah, so that's generally what we  
6   hear a lot, you go out and you talk to different  
7   groups about disinformation that's just a common  
8   theme that we would hear from people that we  
9   should be doing.

10           And as I mentioned, the rest of the  
11   quote is -- is -- it's just not a question of  
12   what we should be doing. There's lots of issues  
13   and things like that there. So that's what I  
14   was trying to get across there.

15           (Exhibit No. 52 was marked for  
16   identification.)

17 BY MR. SAUER:

18           Q.    Exhibit 52.

19           A.    52? I've got it.

20           MR. SAUER: How long have we been  
21   on the record.

22           MR. SCOTT: So I have an unofficial  
23   tally of six hours and 32 minutes.

24           MR. SAUER: Okay. Exhibit --

25           MR. GARDNER: I agree.

1 BY MR. SAUER:

2 Q. Exhibit 52, if we go in this  
3 e-mail -- excuse me, there's an e-mail from  
4 Lauren Protentis copying Allison Snell and Geoff  
5 Hale and Rob Schaul to a contact at Google; do  
6 you see that?

7 A. Mm-hmm.

8 Q. And she says, this is in February  
9 17th of 2022; do you see that?

10 A. I do.

11 Q. And she says: Hi Richard, I hope  
12 this e-mail finds you well. The Department of  
13 Treasury has asked our team for an appropriate  
14 POCs -- I assume that means points of contact --  
15 to discuss social media and influence matters.  
16 We would like to make a connection to Google, if  
17 you're amenable; do you see that?

18 A. I do.

19 Q. What -- do you know why Treasury  
20 reached out to CISA to get a contact for -- at  
21 social media platforms to discuss social media  
22 and influence matters?

23 MR. GARDNER: Objection, lack of  
24 foundation.

25 A. I -- I don't know why Treasury



1 reached out, but CISA obviously, as we discussed  
2 earlier, has points of contact in various social  
3 media companies.

4 Q. Does that happen from time to time,  
5 that other agencies would reach out to CISA and  
6 say: Can you put us in touch with a social  
7 media contact?

8 A. It's -- it's happened a couple  
9 times. I don't -- I don't -- I don't recall how  
10 many, and it's -- it's been awhile, I think,  
11 but -- so if that qualifies as time to time.

12 Q. Do you know what Lauren Protentis  
13 meant when she talked about social media  
14 influence matters, do you know what that means?

15 MR. GARDNER: Objection, calls for  
16 speculation.

17 A. Yeah, I don't know what she means.

18 Q. Were you on detail when this e-mail  
19 was sent?

20 A. I was.

21 Q. Do you remember any discussions  
22 with anyone about the Department of Treasury  
23 reaching out to discuss -- I'm sorry -- wanting  
24 to be put in place in contact with social media  
25 platforms?

1 A. I don't, no.

2 Q. There's a follow up e-mail from  
3 Ms. Protentis, saying: Apologies for the second  
4 e-mail, this is somewhat time sensitive. Do you  
5 know why Treasury was raising a time sensitive  
6 concern -- concern?

7 MR. GARDNER: Objection, calls for  
8 speculation.

9 A. I don't know.

10 Q. Do you know if Treasury ever  
11 connected with the social media platform?

12 A. I don't know.

13 (Exhibit No. 46 was marked for  
14 identification.)

15 BY MR. SAUER:

16 Q. I'm pulling up Exhibit 46. It  
17 should be in the second e-mail I sent you a  
18 moment ago.

19 A. I got it.

20 Q. Here's a draft report to the CISA  
21 director, dated June 22nd, 2022; correct?

22 A. Yes.

23 Q. This is from the CISA cyber  
24 security advisory committee; correct?

25 A. It appears so, yep.

1 Q. I believe you said in your  
2 interrogatory responses that this also has an  
3 MDM subcommittee; is that right?

4 A. Yes, that's correct.

5 Q. Do you participate in those  
6 committees, either the security advisory  
7 committee or the MDM subcommittee?

8 A. I don't.

9 Q. Who participates from -- does  
10 anyone participate from the MDM team in those --  
11 those committees?

12 A. Not from the MDM team, no.

13 Q. So no one on the MDM team  
14 participates in the committees?

15 A. No.

16 Q. Who from CISA participates, do you  
17 know?

18 A. Kim Wyman is, as I mentioned  
19 earlier, I think, that was one of her  
20 responsibilities, and then Geoff Hale  
21 participated.

22 Q. And then who else, from outside  
23 CISA, participates in these meetings?

24 MR. GARDNER: Objection, lack of  
25 foundation.

1           A.    I don't know who's -- I don't know  
2    who's in the -- the participant list. I believe  
3    it's all publicly available online.

4           **Q.    Turning to the second page of this**  
5    **document.**

6           A.    Okay. Recommendations?

7           **Q.    Yeah. First bullet point, do you**  
8    **see there, it says: CISA should focus on MD --**  
9    **I assume that's mis and disinformation?**

10          A.    Is that a question?

11          **Q.    Yeah. Is that --**

12                   MR. GARDNER: Objection, calls for  
13    speculation, lack of foundation.

14    BY MR. SAUER:

15           **Q.    Does MD refer to mis and**  
16    **disinformation?**

17          A.    In the context, I would say that it  
18    does, but I don't -- I don't know what they  
19    meant by it.

20           **Q.    It says: CISA should focus on MD**  
21    **that risks undermining critical functions of**  
22    **American society, including sub-bullet one, MD**  
23    **that suppresses election participation or**  
24    **falsely undermines confidence in election**  
25    **procedures and outcomes; correct?**

1 A. Correct.

2 Q. So the advisory committee is  
3 recommending that CISA focus on election-related  
4 disinformation; right?

5 MR. GARDNER: Objection, lack of  
6 foundation.

7 A. That's how I would read that  
8 sentence, correct.

9 Q. Okay. Second bullet point says:  
10 MD that undermines critical functions carried  
11 out by other key democratic institutions, such  
12 as the courts or by other sectors, such as the  
13 financial system or public health measures;  
14 right?

15 A. That's what it says, yep.

16 Q. You talked about the financial  
17 system, earlier, and interestingly that's raised  
18 in this recommendation. Are you aware of CISA  
19 doing anything to address MD that undermines the  
20 financial system?

21 A. So we've -- as I mentioned earlier,  
22 we -- we're working with Treasury to develop a  
23 product to help the financial services sector  
24 understand MDM risks to the sector.

25 Q. What risks have there been to that

1       **sector? And I don't remember any runs on banks,**  
2       **you know, recently, what risks?**

3               A.     So again, as I mentioned earlier,  
4       we're not the experts in financial services, so  
5       we, you know, depend on the financial services  
6       sector to kind of work us through, help us work  
7       through what those risks are, we're pretty early  
8       in the process, so we're still kind of working  
9       through those sorts of questions.

10              **Q.     Do you know what, what was the**  
11       **impetus for doing that product in the first**  
12       **place? Was someone worried about MDM that would**  
13       **undermine financial services?**

14              A.     I -- I don't -- I don't know why  
15       Treasury reached out to us and discussed that, I  
16       don't recall.

17              **Q.     Is that unrelated to the last**  
18       **e-mail we saw, where they wanted to talk to**  
19       **social media platforms about social media and**  
20       **influence matters?**

21                      MR. GARDNER: Objection, calls for  
22       speculation, lack of foundation.

23              A.     Yeah, I don't know. I don't know  
24       if the two are connected.

25              **Q.     Okay. The bottom of the same page,**

1       there's a bullet recommending that CISA should  
2       consider MD across the information ecosystem;  
3       right?

4               A.     Yep.

5               Q.     And it goes down in the second  
6       sub-bullet there, it says: CISA should approach  
7       the MD problems with the entire information  
8       ecosystem in mind, this includes social media  
9       platforms of all sizes, mainstream media, cable  
10      news, hyper partisan media, talk radio and other  
11      online resources; do you see that?

12              A.     I do.

13              Q.     Has CISA been taking steps to  
14      consider or address misinformation in these  
15      other venues, besides social media, for example,  
16      mainstream media?

17              A.     No. What I would say is that,  
18      generally speaking, we -- we -- I believe it's  
19      generally too much of a focus on just the social  
20      media platform, and MDM that kind of flows  
21      through social media. When potentially it's MDM  
22      that flows through all different sources of  
23      media communication.

24                      So that's kind of how we think  
25      about it, we try not to just focus on MDM, but

1 we don't do anything counter to your point.  
2 Again, we built resilience helping people  
3 understand what's going on and how to mitigate  
4 the risks.

5 **Q. Do you try to build resilience to**  
6 **MDM on -- in cable news?**

7 A. I mean, generically speaking, all  
8 of our resilience activity would be useful  
9 regardless of how -- we try to make it as broad  
10 as possible so it's applicable anywhere that  
11 somebody may come across MDM.

12 **Q. How about hyper partisan media,**  
13 **what does that mean, do you know?**

14 MR. GARDNER: Objection, calls for  
15 speculation.

16 A. I don't know what it's meant in  
17 this context, but again, we try to be general  
18 enough in our kind of guidance to help people  
19 understand.

20 We're essentially agnostic of where  
21 it's coming from, we just want people to be able  
22 to understand where -- what it is, how it works,  
23 and things they can do to mitigate those risks.

24 **Q. I take it, then, the MDM team would**  
25 **agree with this recommendation that CISA should**



1        **approach the MDM problem, you know, with a whole**  
2        **information universe in mind, including**  
3        **mainstream media, cable news, hyper partisan**  
4        **media, talk radio, and other online resources?**

5                    MR. GARDNER: Objection, form.

6                    A.    What I would say, from a  
7        resilience-building standpoint, we generally  
8        don't -- try not to hone too much on any one  
9        particular medium for communication. There's  
10       obviously tactics that fall across multiple, but  
11       we don't generally try to hone in on any one in  
12       particular.

13                    (Exhibit No. 59 was marked for  
14       identification.)

15       BY MR. SAUER:

16                    Q.    I'm pulling up Exhibit 59.

17                    A.    Okay.

18                    Q.    **And then here's a cyber security**  
19        **advisory committee e-mail to a group, I assume**  
20        **it's the committee members; does that look right**  
21        **to you or do you not know?**

22                    MR. GARDNER: Objection, lack of  
23        foundation, calls for speculation.

24                    A.    Yeah, I don't -- I don't know who  
25        all the members are, so it would be hard for me

1 to say if that's the case.

2 Q. Here's some people that are copied  
3 on this e-mail from the CISA cyber security  
4 advisory committee e-mail, the first one is Kate  
5 Starbird; right?

6 A. Yeah.

7 Q. Do you know who she is?

8 A. She's a professor at the University  
9 of Washington.

10 Q. She was involved in the Election  
11 Integrity Partnership that we talked about  
12 earlier; right?

13 A. I believe so, yeah.

14 Q. Next one is Vijaya Gadde or Gadde,  
15 do you know who she is?

16 A. I don't know.

17 Q. Was she a senior official at  
18 Twitter, at the time, do you know?

19 MR. GARDNER: Objection, calls for  
20 speculation.

21 A. I don't know.

22 Q. I see you've got Kim Wyman and  
23 Geoff Hale on this e-mail. They were the two  
24 that you testified earlier are involved in the  
25 cyber security advisory committee for CISA;

1 right?

2 A. Yep.

3 Q. And then lower down, there's a list  
4 of -- we have identified a list of potential  
5 subject matter experts to potentially brief at  
6 our biweekly meetings, bios attached; do you see  
7 that?

8 A. I do.

9 Q. So -- and that's a list of, I take  
10 it, experts who would provide briefings at the  
11 advisory committee's meetings; is that how you  
12 read that?

13 MR. GARDNER: Objection, lack of  
14 foundation, calls for speculation.

15 A. So the paragraph reads: Identify a  
16 list of subject matter experts. Please be  
17 prepared to provide your feedback. I'm sorry,  
18 what was your question again?

19 Q. Let me just ask: Is the third  
20 expert on the list is Renée DiResta; right?

21 A. Yeah.

22 Q. And she's at Stanford Internet  
23 Observatory; right?

24 A. Correct.

25 Q. You were involved in conversations

1       **with her, because she was a part of the Election**  
2       **Integrity Partnership; right?**

3               A.    We should have Stanford Internet  
4       Observatory, we were certainly involved in  
5       conversations with her, as I talked about  
6       earlier.

7               **Q.    And those conversations were**  
8       **related to the commencement of the Election**  
9       **Integrity Partnership; right?**

10              A.    I -- I don't know if she was  
11       involved in the early conversations, before it  
12       stood up. I know Stamos was there, I don't know  
13       if Renée was there in those early conversations.

14              **Q.    Was she in some conversations**  
15       **between -- with you about the EIP?**

16              A.    As I mentioned before, she briefed  
17       us about the 2022 EIP work. I don't recall  
18       conversations in 2020, but again, it wouldn't  
19       surprise me if she was involved in those.

20              MR. SAUER:  Let's go off the  
21       record.

22              THE VIDEOGRAPHER:  The time is now  
23       5:46 p.m. We are off the record.

24              (Recess.)

25              THE VIDEOGRAPHER:  The time is now

1 5:53 p.m. We're back on the record.

2 MR. SAUER: Are we back on the  
3 record?

4 THE VIDEOGRAPHER: Yes.

5 MR. SAUER: Oh, sorry.

6 (Exhibit No. 19 was marked for  
7 identification.)

8 BY MR. SAUER:

9 Q. Exhibit 19, I put it on the screen  
10 share.

11 Here's a proposal from CIS, Center  
12 For Internet Security, to create an election  
13 misinformation reporting portal, and it talks  
14 about the benefits to election officials being  
15 in a single place for reporting mis and  
16 disinformation across multiple social media  
17 platforms.

18 Do you know if this proposal was  
19 ever implemented to create a single election  
20 misinformation reporting portal?

21 A. I -- I don't know. I'm not  
22 entirely sure. I don't know that I've seen  
23 this, I don't know if I've seen this proposal  
24 before, so I'm not certain.

25 Q. So you don't know?

1           A.    It sounds like what they were  
2   trying to do, that we discussed earlier, but I  
3   don't know to what extent it was, to your  
4   question, to what extent it was stood up or  
5   established.

6           **Q.    You don't know to what extent that**  
7   **CIS managed to implement this proposal for an**  
8   **elections misinformation reporting portal?**

9           A.    Yeah, or if they -- if they did it  
10   at all.

11                           (Exhibit No. 21 was marked for  
12   identification.)

13   BY MR. SAUER:

14           **Q.    Exhibit 21, it's on the screen**  
15   **share, this is a CNN political report, September**  
16   **of 2022. If you go to the third -- fourth page**  
17   **of the document, in this report it says: While**  
18   **the anti-doxing and foreign influence parts of**  
19   **the proposal remain stalled, work on the online,**  
20   **quote, portal for election officials to flag**  
21   **misinformation to social media platforms**  
22   **predated the proposal and continues today,**  
23   **according to people familiar with it.**

24                           So are you aware of ongoing work,  
25   at least as of September of 2022, to set up an

1       **online portal for election officials to flag**  
2       **misinformation to social media platforms.**

3               A.     So I think as I testified to  
4       earlier, my understanding is that CIS did do  
5       something along the lines, I just don't know the  
6       extent of it.

7               **Q.     And you don't know whether or when**  
8       **it -- it might be completed?**

9               A.     Correct.

10               (Exhibit No. 24 was marked for  
11       identification.)

12       BY MR. SAUER:

13               **Q.     Exhibit 24, here's a CISA bulletin**  
14       **that's on your website called --**

15               A.     Mm-hmm.

16               **Q.     -- misinformation, you go to the**  
17       **third page.**

18               A.     Correct.

19               **Q.     Are you familiar with this**  
20       **bulletin?**

21               A.     Actually, I think this may be our  
22       website. I'm not sure if it's a bulletin.

23               **Q.     It is on your website. I don't**  
24       **know if it's a bulletin, either.**

25               **Let me ask you this: Here on the**

1        **third page, it says: Bridging election**  
2        **stakeholders and social media, and under there**  
3        **it says: The MDM team serves as a switchboard**  
4        **for routing disinformation concerns to**  
5        **appropriate social media platforms and law**  
6        **enforcement; correct.**

7            A.    It does, yep.

8            **Q.    You guys refer stuff to law**  
9        **enforcement, too?**

10           A.    Yes, if there was -- particularly  
11        if there was violence, promoted in whatever was  
12        sent to us from an election official.

13           **Q.    Anything else involved that would**  
14        **be reported to law enforcement, other than**  
15        **threats of violence?**

16           A.    So we would generally share  
17        whatever we received from the election officials  
18        with the FBI, in case there was an ongoing  
19        investigation related to whatever it was that we  
20        forwarded to them.

21           **Q.    And is this still true, I mean,**  
22        **it's on your website today, is it still true**  
23        **that the MDM team serves as a switchboard for**  
24        **routing disinformation concerns to appropriate**  
25        **social media platforms?**



1 A. No. Like I said earlier, we didn't  
2 do this in 2022, so we should change that to  
3 served. Thank you for finding that.

4 Q. And I take it you -- you testified  
5 earlier that that decision was made in late  
6 April or early May of 2022?

7 A. That's my recollection.

8 Q. Do you know why the decision was  
9 made?

10 A. I don't, but as I also mentioned,  
11 it was something that we were comfortable with,  
12 from the MDM team perspective, because of heavy  
13 burden on our resources.

14 Q. You anticipate serving in a  
15 switchboard in the future or do you not know  
16 whether you will?

17 A. That's not my decision to make,  
18 so -- so I don't want to speak on behalf of the  
19 director or future directors.

20 Q. You don't know what the director's  
21 plans are for the future when it comes to  
22 serving as a switchboard for routing  
23 disinformation concerns?

24 A. I don't know what direct --  
25 Director Easterly's position is, and obviously I

1 wouldn't know any future director's position on  
2 that, either.

3 (Exhibit No. 6 was marked for  
4 identification.)

5 BY MR. SAUER:

6 Q. Exhibit 6?

7 A. Okay.

8 Q. Here's a public comments by Renée  
9 DiResta about -- about the Election Integrity  
10 Project. And let me put it on the screen share.

11 On the third page, call -- which is  
12 called page 2 of the transcript, she talks -- or  
13 sorry, it's quoting Alex Stamos, saying that the  
14 EIP started with our team at Stanford sending a  
15 group of interns to work with CISA; right? Do  
16 you see that?

17 A. Yep.

18 Q. It talks about the sort of stuff we  
19 talked about the gap earlier, about how there's  
20 a lack of capability, about disinformation.

21 But Stamos says they lack a funding  
22 and legal authorization to do the kinds of work  
23 that will be necessary to truly understand how  
24 election disinformation was operated; correct?

25 A. That's what he says, yep.

1 Q. And he goes on to say: Our  
2 partners in government, most particularly those  
3 in CISA and DHS, but also state and local  
4 governments whom we worked with; correct?

5 A. He says that, yes.

6 Q. Were CISA and DHS partners of the  
7 EIP, in your view?

8 A. We generally describe any external  
9 organization that we have a relationship as a  
10 partner. So I think that probably, you know --  
11 so yeah.

12 Q. Okay. So in a sense that you were  
13 a partner of the EIP, fair to say?

14 A. Again, we would say that of any  
15 external entity that we have a relationship  
16 with.

17 (Exhibit No. 7 was marked for  
18 identification.)

19 BY MR. SAUER:

20 Q. On the screen share I put Exhibit  
21 7, which is now public comments from Renée  
22 DiResta from the EIP; do you see it up there?

23 A. Sorry, you are an on Exhibit 7?

24 Q. Yeah.

25 A. Yep.

1 Q. If you go to page 2 of the  
2 transcript, which is page 4 of the PDF, and  
3 it -- it quotes Renée DiResta, again, talking  
4 about the students from Stanford doing an  
5 internship at CISA and identifying a gap, right,  
6 that was the word we used earlier?

7 A. Mm-hmm.

8 Q. It talks about how there was no  
9 clear federal lead to coordinate, and it wasn't  
10 prepared to identify it; correct?

11 A. I don't --

12 Q. It says that gap, the federal  
13 government wasn't prepared to identify and  
14 analyze election mis and disinfo; correct?

15 A. Correct. That's what she says,  
16 yep.

17 Q. And she says there was no clear  
18 federal lead to coordinate the work and so  
19 forth?

20 A. Correct.

21 Q. And she says: There were unclear  
22 legal authorities, including very clear first  
23 amendment questions; right?

24 A. That's what she says.

25 Q. That's a reference to the federal

1 government taking the leadership role and  
2 analyzing to respond to election mis and  
3 disinformation; correct?

4 A. I'm not seeing that in here, is  
5 that a sentence or are you asking me to --

6 Q. I'm just --

7 A. -- interpret what Renée is saying?

8 Q. Yeah, interpret, is that how you  
9 read it? That's how I read it.

10 MR. GARDNER: I'm sorry, can you --  
11 John, can you re-ask that question?

12 BY MR. SAUER:

13 Q. Let me ask you this: Were there  
14 any discussions of -- that you're aware of,  
15 relating to the EIP, that related to unclear  
16 legal authorities, including very real first  
17 amendment questions, when it comes to direct  
18 involvement of the federal government?

19 A. I'm not aware, but, in general,  
20 conversations about MDM, first amendment comes  
21 up.

22 Q. Did it come up with the CISA  
23 interns who originated the idea of the EIP?

24 A. I don't -- I don't recall that  
25 being the nature of the conversation. I think

1 it was really mostly around gaps for election  
2 officials. But as you probably picked up, I  
3 don't remember in detail the conversations that  
4 well that long ago.

5 MR. SAUER: I think that's all the  
6 questions I have.

7 MR. GARDNER: Well, the government  
8 has no questions. We just, again, we emphasize  
9 that the witness will read and sign.

10 THE VIDEOGRAPHER: This  
11 concludes -- this concludes the deposition of  
12 Brian Scully. The time is now 6:04 p.m. We are  
13 off the record.

14 THE REPORTER: Mr. Sauer, when do  
15 you need the transcript?

16 MR. SAUER: Could we have it  
17 expedited within two days, that's -- Ben, I  
18 think our standard request for these is two  
19 business days?

20 MR. GARDNER: Yes.

21 THE REPORTER: And Mr. Gardner,  
22 will you be purchasing a copy.

23 MR. GARDNER: Yes, ma'am, we'll be  
24 purchasing a copy.

25 THE REPORTER: And you want the

1 same delivery?

2 MR. GARDNER: Yes, ma'am.

3 THE REPORTER: Is it okay if I  
4 e-mail you spelling questions on Monday?

5 MR. GARDNER: You have until  
6 Tuesday, with the holiday.

7 (Signature having not been waived,  
8 the deposition of BRIAN SCULLY was concluded at  
9 6:04 p.m.)

10 ACKNOWLEDGMENT OF DEPONENT

11 I, BRIAN SCULLY, do hereby acknowledge  
12 that I have read and examined the foregoing  
13 testimony, and the same is a true, correct and  
14 complete transcription of the testimony given by  
15 me and any corrections appear on the attached  
16 Errata sheet signed by me.

17

18

19 \_\_\_\_\_  
(DATE)

\_\_\_\_\_  
(SIGNATURE)

20

21

22

23

24

25

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25

CERTIFICATE OF SHORTHAND REPORTER

I, Cassandra E. Ellis, Registered Professional Reporter, the officer before whom the foregoing proceedings were taken, do hereby certify that the foregoing transcript is a true and correct record of the proceedings; that said proceedings were taken by me stenographically and thereafter reduced to typewriting under my supervision; and that I am neither counsel for, related to, nor employed by any of the parties to this case and have no interest, financial or otherwise, in its outcome.

IN WITNESS WHEREOF, I have hereunto set my hand this 17th day of January 2023.

*Cassandra E. Ellis, CSR*

\_\_\_\_\_  
CASSANDRA E. ELLIS, CSR-HI, CSR-VA, CCR-WA, RPR,  
CRR  
REALTIME SYSTEMS ADMINISTRATOR  
NOTARY PUBLIC



**BRIAN J. SCULLY 1/12/2023**

**Page 375**

1 LEXITAS LEGAL

2

3 January 17, 2023

4

5 JOSHUA E. GARDNER, ESQUIRE  
6 DEPARTMENT OF JUSTICE  
7 1100 L STREET, NORTHWEST  
8 WASHINGTON, D.C. 20530

7

8 IN RE: THE STATE OF MISSOURI, et al. v. JOSEPH R.  
9 BIDEN, JR., et al.

9

10 Dear JOSHUA E. GARDNER:

11 Please find enclosed your copies of the deposition of  
12 BRIAN J. SCULLY taken on January 12, 2023 in the  
13 above-referenced case. Also enclosed is the original  
14 signature page and errata sheets.

15 Please have the witness read your copy of the  
16 transcript, indicate any changes and/or corrections  
17 desired on the errata sheets, and sign the signature  
18 page before a notary public.

19 Please return the errata sheets and notarized  
20 signature page within 30 days to our office at 1608  
21 Locust Street, Kansas City, MO 64108 for filing.

22 Sincerely,

23

24 Lexitas Legal

25 Enclosures

**BRIAN J. SCULLY 1/12/2023**

1	ERRATA SHEET
2	Witness Name: BRIAN J. SCULLY
3	Case Name: THE STATE OF MISSOURI, et al. v. JOSEPH R. BIDEN, JR., et al.
4	Date Taken: JANUARY 12, 2023
5	Page # _____ Line # _____
6	Should read: _____
7	Reason for change: _____
8	
9	Page # _____ Line # _____
10	Should read: _____
11	Reason for change: _____
12	
13	Page # _____ Line # _____
14	Should read: _____
15	Reason for change: _____
16	
17	Page # _____ Line # _____
18	Should read: _____
19	Reason for change: _____
20	
21	Page # _____ Line # _____
22	Should read: _____
23	Reason for change: _____
24	
25	Witness Signature: _____

**BRIAN J. SCULLY 1/12/2023**

1 STATE OF \_\_\_\_\_ )

2

3 COUNTY OF \_\_\_\_\_ )

4

5 I, BRIAN J. SCULLY, do hereby certify:

6 That I have read the foregoing deposition;

7 That I have made such changes in form

8 and/or substance to the within deposition as might

9 be necessary to render the same true and correct;

10 That having made such changes thereon, I

11 hereby subscribe my name to the deposition.

12 I declare under penalty of perjury that the

13 foregoing is true and correct.

14 Executed this \_\_\_\_\_ day of \_\_\_\_\_,

15 20\_\_\_\_, at \_\_\_\_\_.

16

17

18

19

\_\_\_\_\_

20

BRIAN J. SCULLY

21

22

\_\_\_\_\_

23

NOTARY PUBLIC

24 My Commission Expires:

25

**BRIAN J. SCULLY 1/12/2023**

<b>A</b>	205:24	105:3,5	<b>addition</b>	<b>administ...</b>
<b>A-a-r-o-n</b>	206:7,22	130:17	75:9	234:25
103:6	207:8	137:20	184:13	<b>Administ...</b>
<b>A-l-e-x</b>	230:13	278:25	235:23	2:8 374:20
167:6	281:3,22	304:5	<b>additional</b>	<b>admonition</b>
<b>A-y-e-l-e-t</b>	298:3,4	312:12	40:22 41:3	196:7
187:18	<b>accurate</b>	325:8	88:14	<b>adopt</b> 132:18
<b>a.m</b> 1:16	290:22	329:15	209:17	<b>adversarial</b>
10:4	291:5	331:17	210:3	270:17,22
226:19	315:13	332:14	220:7,17	271:5
<b>Aaron</b> 103:2	<b>acknowledge</b>	<b>activity</b>	222:19	<b>advisor</b>
103:5,6	373:11	64:25	303:9,24	195:19
112:16,17	<b>ACKNOWLE...</b>	152:10	337:17	305:5
112:17	373:10	166:1	<b>Addition...</b>	<b>advisory</b>
157:19,21	<b>acronym</b>	358:8	117:25	37:17
157:21	307:24	<b>actor</b> 37:23	<b>address</b>	352:24
217:4	<b>acronyms</b>	259:14	66:15	353:6
227:18	307:24	270:17,22	120:8,12	355:2
<b>abbrevia...</b>	<b>act</b> 35:6	<b>actors</b> 27:12	120:13	359:19
316:24	229:6	27:21 38:1	128:11	360:4,25
<b>ability</b>	240:3	38:2,4,8	131:18	361:11
92:24,25	<b>acted</b> 165:13	38:10,12	137:21	<b>advocating</b>
93:19 94:6	<b>acting</b> 121:3	39:21	157:5	132:17
94:11,17	<b>action</b> 94:12	246:2	198:21	<b>aegis</b> 73:22
<b>able</b> 358:21	95:14	256:20	203:19	<b>affect</b> 57:21
<b>above-re...</b>	177:9,13	271:6	205:6	340:25
375:13	178:6,6	273:24	320:8	<b>affirmative</b>
<b>absence</b> 19:5	200:14	323:23	324:12	347:10
20:6	288:11	<b>actual</b> 36:19	328:24	<b>Afghanistan</b>
<b>absolutely</b>	<b>actioned</b>	61:16	348:20	322:2
287:22	164:10	155:15	355:19	324:21
<b>academia</b>	165:3	193:15	357:14	<b>afraid</b>
44:6	168:14	255:11	<b>addressed</b>	292:10,17
<b>academic</b>	177:4	258:10	163:20	307:20
46:10,21	<b>actions</b> 40:9	270:25	<b>addresses</b>	<b>afternoon</b>
47:2	40:15,25	274:5	214:19,24	163:7
<b>accident...</b>	240:8	275:2	<b>addressing</b>	173:17,19
262:4	242:4	343:22	58:24	176:1
<b>accidently</b>	279:5	<b>Adam</b> 33:12	151:7	284:23,25
293:8	<b>active</b> 19:9	276:20	278:12	<b>afters</b>
<b>account</b>	33:24	<b>add</b> 171:2	322:6	122:20
206:17	125:22	290:4	332:5	<b>agencies</b>
207:5	137:20	297:2	<b>administ...</b>	25:11,17
230:13	<b>actively</b>	300:8,12	25:3	25:22
281:11,18	287:18,18	331:7	<b>administ...</b>	37:12
294:9,13	<b>activities</b>	337:15	25:4	73:11,16
295:11	16:8 21:14	<b>adding</b>	239:16	73:21 92:2
296:21	43:21	119:14	313:16,22	92:10,14
<b>accounts</b>	69:22 90:9	336:21	314:4,10	92:25

**BRIAN J. SCULLY 1/12/2023**

93:20	272:21	293:14	<b>alleged</b>	<b>analyses</b>
95:15	275:3,24	297:7	200:3	125:24
136:24	<b>agents</b>	298:19	217:8	<b>analysis</b>
245:25	220:11	302:4,15	225:16	16:22 26:3
246:13	<b>agnostic</b>	315:21	<b>Alliance</b>	43:20,21
250:5,17	358:20	348:17	47:7	43:24
250:21	<b>ago</b> 101:5	<b>aided</b> 118:1	<b>Allison</b> 28:8	59:16 60:6
256:5	295:15	118:15	253:16	60:17
258:3,11	352:18	<b>aimed</b> 17:5	350:4	123:1
262:19	372:4	<b>al</b> 1:6,10	<b>allow</b> 151:14	144:16,16
264:17	<b>agree</b> 42:5,7	10:6,8	289:2	147:6,9
267:6,19	95:19	375:8,8	<b>allows</b> 148:4	172:1
314:15	349:25	376:3,3	<b>alternate</b>	187:15
315:2	358:25	<b>alert</b> 27:5	62:21	225:13
317:12	<b>agreed</b> 86:20	<b>Alethia</b>	345:10	333:24
327:15	<b>agreement</b>	47:14	<b>alternative</b>	<b>analyst</b>
351:5	2:2 212:7	<b>Alex</b> 43:14	344:15	28:19
<b>agency</b> 4:7	<b>ahead</b> 8:18	70:5,14	<b>amenable</b>	43:14,16
8:12 15:25	53:12 73:5	72:16 76:9	350:17	167:25
72:2 90:17	87:23	76:14,15	<b>amended</b> 6:22	171:18
91:5 94:21	89:14	77:8,17	190:18	<b>analysts</b>
95:5	113:3	86:2 88:8	<b>amendment</b>	108:12
141:24	122:2	89:6 99:10	95:14	109:18,22
178:11	124:8	102:2	153:5	187:10
248:10	126:11	111:22	370:23	<b>analysts'</b>
250:23	141:15	116:21,24	371:17,20	29:3
251:2	144:6	117:2,8,16	<b>American</b>	<b>analytic</b>
284:16	146:20	134:21	46:25	44:12
286:14	161:23	136:5,9,13	341:24	184:4
315:9	162:5	136:15	354:22	<b>analyze</b>
316:18,24	173:2,9	139:7,11	<b>Americans</b>	182:9
317:3	195:4	139:21,23	280:11,20	370:14
335:19	203:25	142:12	280:23	<b>analyzing</b>
343:15,17	204:5	166:19	344:23	371:2
<b>agenda</b> 21:9	215:21	167:3,6	346:12,17	<b>and/or</b>
30:18,20	218:14,15	171:11,12	347:24	375:16
30:22,23	221:7	171:14	<b>amount</b> 50:23	377:8
34:5	222:8,10	179:18	346:11,17	<b>Announce...</b>
128:14,15	225:20	181:10,14	347:16,23	8:15
129:2	256:24	182:17,17	<b>amplific...</b>	<b>announces</b>
169:9	257:10	184:14	287:6,8	217:11
234:17	261:24	185:2,4,12	288:24	<b>announcing</b>
256:3	266:25	191:25	<b>amplified</b>	35:9
257:15,23	269:4	192:12	287:10,13	<b>answer</b> 13:1
260:5	271:9	196:24	<b>amplify</b>	34:19 35:5
262:8	273:8	197:7	254:18	51:2 53:3
269:6,14	285:15	198:19	347:11,21	71:23 80:7
270:6,25	288:15	199:6,16	<b>Amplifying</b>	93:4 133:3
272:5,8,18	289:9	368:13	346:23	133:23

**LEXITAS LEGAL**

**BRIAN J. SCULLY 1/12/2023**

148:10	14:4 55:7	256:9	319:20	94:10
150:22,22	107:11	257:19	320:6,22	100:20
152:24	282:2	258:4	321:11	107:1
153:10,20	<b>appear</b> 82:25	<b>approaching</b>	336:3	128:9
153:21	205:23	163:11	338:14	130:21
156:2,11	373:15	<b>appropriate</b>	<b>articles</b>	132:24,25
162:1	<b>appeared</b>	17:7 95:15	124:2,5,13	133:4
163:13	225:15	315:16	<b>articulate</b>	135:11,11
167:13	<b>appearing</b>	350:13	311:4	137:1
180:24	192:10	366:5,24	<b>articulated</b>	156:3
185:9	<b>appears</b>	<b>April</b> 22:3,6	239:7	172:15
198:14	159:17	22:7,16,20	<b>artifact</b>	222:18
202:21	162:23	22:25 23:9	60:3	228:24
237:20	173:15	23:11	<b>Ashwin</b>	249:3
250:6	192:15	260:3	187:20	256:13
278:21,21	196:16	262:1	<b>asked</b> 63:13	261:19
292:10,17	199:25	294:14	101:9	277:7
304:24	200:1	336:13	126:5	287:12
310:15	207:23	367:6	136:13,23	292:12
339:15,18	211:20	<b>April-ish</b>	140:6	295:18,19
339:18,22	226:10	12:6	146:16	297:1,4
<b>answered</b>	228:22	<b>April/May</b>	147:13	301:5
126:6	230:16	12:6	161:25	348:8,23
146:17	277:10	<b>area</b> 241:25	163:22	371:5
162:1	281:12	<b>areas</b> 312:23	202:16	<b>asks</b> 100:23
202:16	282:18	313:5	218:23	232:6
230:20	285:9	<b>argue</b> 338:16	219:4	261:16
251:3,8	292:2	<b>Arizona</b>	220:18,20	<b>assembled</b>
<b>answering</b>	297:4	225:7,18	223:3	97:7
339:20	301:13	<b>Arizona's</b>	230:19	<b>assembling</b>
<b>answers</b>	352:25	225:2	250:4,15	97:14
150:19	<b>applicable</b>	<b>arose</b> 147:4	251:1,6	<b>assembly</b>
<b>anti-doxing</b>	358:10	<b>arrangement</b>	260:8,20	97:16
364:18	<b>applied</b>	121:9	261:15	<b>asserted</b>
<b>anticipate</b>	224:17	187:2	270:4	166:12
256:9,15	<b>applies</b>	<b>arranging</b>	284:4	<b>assess</b>
367:14	153:1	214:1	296:16	144:18
<b>anticipated</b>	260:24	<b>arrived</b> 86:8	301:11,16	<b>assessed</b>
258:5,13	<b>apply</b> 17:17	<b>arrives</b>	307:10	109:22
<b>anticipa...</b>	<b>appointee</b>	14:25	318:22	<b>assessing</b>
257:19	130:4,8,12	<b>arrow</b> 105:16	350:13	96:10,18
<b>anybody</b>	313:15,17	105:17	<b>asking</b> 13:11	123:8
129:14	<b>approach</b>	106:17	13:23 57:3	<b>assessments</b>
<b>API</b> 146:7,9	39:15 85:9	<b>article</b> 8:7	66:24 74:7	257:3
146:13,13	97:5 307:5	8:11,16	74:10	<b>assignment</b>
146:14	307:12	9:5,15	91:10	19:19
<b>Apologies</b>	357:6	304:6,17	92:11,12	<b>assist</b>
352:3	359:1	305:22	92:13 93:6	322:22
<b>apologize</b>	<b>approaches</b>	314:19	93:14 94:9	<b>assistance</b>

**BRIAN J. SCULLY 1/12/2023**

101:10	<b>atlassia...</b>	273:22,24	<b>awake</b> 175:9	326:12
<b>assistant</b>	205:15	274:3,4,8	<b>aware</b> 17:13	328:19
195:11	<b>attached</b> 5:7	274:10	17:16 18:1	329:19,22
196:14	6:2 7:2	275:7,11	52:2 61:22	332:17
311:17	8:2 9:2	275:14,19	75:5,12	336:4,20
<b>assisting</b>	253:1	<b>attribut...</b>	77:6,7,22	355:18
84:25	361:6	273:19	78:17,18	364:24
<b>associated</b>	373:15	274:25	79:3 80:22	371:14,19
135:7	<b>attachments</b>	<b>Audio</b> 5:14	106:21	<b>awareness</b>
146:2	345:15	5:18	107:3,6,8	16:12
246:20	<b>attacks</b>	<b>audit</b> 17:3	112:18	17:11
<b>Association</b>	246:21,22	334:5	124:22	21:15
50:8,9	<b>attempt</b> 66:4	<b>August</b> 9:23	127:5,10	65:15
101:16,18	134:11	15:9	128:8,12	68:17
101:19	211:25	104:25	129:16,18	131:6
103:13	317:18	262:8	132:8,10	155:7
<b>Assortment</b>	337:14	277:4	133:8,11	267:17,25
6:4,13	<b>attempted</b>	302:22	138:13	268:2
7:12,17	254:17	303:2,5	147:14,23	325:25
<b>assume</b> 20:12	<b>attempts</b>	328:21	152:3	326:2
105:6	254:11	334:5	158:4,17	347:25
166:6	<b>attend</b> 264:2	<b>authenti...</b>	160:10	<b>awful</b> 55:6
177:18	<b>attended</b>	223:6,25	163:8	<b>awhile</b> 344:3
180:6	259:20,23	<b>authorities</b>	164:5	351:10
205:20	<b>attention</b>	85:1 91:20	172:9,14	<b>Ayelet</b>
219:19	15:2,15	92:10	188:10	186:17,20
226:12	17:23 18:2	93:16	196:17	187:17
274:9	20:23	278:15	197:13	
275:9	69:25	370:22	202:19,21	<b>B</b>
309:6	173:1	371:16	202:22,23	<b>B</b> 5:6 6:1
350:14	196:21	<b>authority</b>	203:6	7:1 8:1
354:9	197:20	26:19	207:12	9:1 219:1
359:19	203:3	91:17 92:1	211:4,22	<b>B-e-e-b-e</b>
<b>assumed</b>	<b>attorney</b> 3:7	92:14,19	215:8	279:21,24
158:21	10:20,23	92:24 94:1	222:5	<b>back</b> 19:12
<b>Assuming</b>	13:18	96:3,24	255:9	19:21
275:15	35:10	337:14	290:9,12	20:23 22:3
<b>assumption</b>	<b>attorneys</b>	<b>authoriz...</b>	290:24	24:9 32:6
118:20	10:17	368:22	295:17,21	33:9,23
230:25	34:12	<b>available</b>	302:17,21	35:3 37:14
243:14	165:18	43:8,13	302:25	42:20
298:15	<b>attributing</b>	82:16	303:5,8	51:14
329:18	273:24	113:15	307:9	58:10
<b>astonishing</b>	275:19	145:1,14	320:7,24	71:25 72:1
276:23	349:3	195:6	321:12	76:6 78:19
<b>Atlanta</b>	<b>attribution</b>	333:12	322:5,11	80:19
48:19	122:25	354:3	322:13	83:13 85:5
<b>Atlantic</b>	272:10	<b>avoid</b> 120:25	324:18,22	106:19,22
5:15	273:15,21	211:25	325:1	107:1

**LEXITAS LEGAL**

**BRIAN J. SCULLY 1/12/2023**

141:1	342:14	222:21	51:7 52:7	224:1
147:9	363:1,2	<b>bathroom</b>	53:4,8,19	233:3
163:19	<b>bad</b> 245:22	319:1	53:22 54:6	238:21
164:4,12	297:17	<b>BCC</b> 308:15	55:5 60:25	241:20
164:17,22	<b>bag</b> 64:9	<b>Beckman</b>	61:2,14	251:3,17
165:8,10	<b>ballots</b>	28:16,22	64:13 67:6	259:7,10
165:10	218:25	<b>Beebe</b> 279:20	67:11	264:8,13
166:16,19	219:2,12	<b>beef</b> 336:4	72:22 73:1	266:2
168:13,17	339:10	<b>beefing</b> 8:12	76:8,11,17	270:2,3
170:11,14	<b>bandwidth</b>	335:20,24	76:22,25	271:4
173:1	57:20	<b>began</b> 183:13	77:20 78:6	278:20,22
176:21	<b>banking</b>	<b>beginning</b>	85:22	281:1
177:12,19	342:7	23:13	88:23 89:3	289:6
179:15	<b>banks</b> 342:7	126:17	90:4 92:23	303:8
180:4	342:10,16	157:11	100:23	308:2
183:9,11	356:1	307:6	111:13	311:20
197:25	<b>based</b> 17:21	<b>begins</b>	112:23	317:2
201:17	41:9,14	125:18	113:1	323:12
209:12	113:15	330:10	119:6	325:12
218:12	114:17	<b>behalf</b> 3:2	120:14	327:3,11
219:22	154:15	3:16 4:2	124:1	327:17
220:12	209:17	10:20 11:1	127:20	353:1
221:4	242:4	16:24 28:2	134:13,22	354:2
223:11	257:14	28:3 35:11	136:3,7	357:18
224:19	272:15	106:11	137:10,23	360:13
229:12	285:9	189:18	139:11,14	<b>believed</b>
231:4,15	292:21	243:12	139:22,25	27:21
232:15	<b>basic</b> 238:16	367:18	143:1	266:5
242:12,19	241:13	<b>behavior</b>	144:23	<b>bell</b> 126:1
243:25	<b>basically</b>	41:23 42:3	151:17,18	197:16
256:13	30:16 45:6	42:10,16	151:19	213:24
259:21,22	56:15	115:2	155:2	247:9
262:13	59:24	176:9	159:20	284:14
263:2	60:22	311:5,6,10	161:16	294:22
267:4	86:24	<b>beings</b> 28:22	164:24	<b>Ben</b> 372:17
274:20	260:22	<b>believe</b>	166:6	<b>benefits</b>
275:2	<b>basis</b> 35:6	19:18 20:2	168:22	363:14
276:10,11	219:15	22:3,13	179:6	<b>Berkman</b>
277:4,14	248:6	24:7,13,19	183:19	345:24
282:1	<b>Bates</b> 6:4,14	26:20	184:19	<b>best</b> 61:9
288:10	6:20 7:8	28:16 29:6	187:1,21	85:9 101:8
289:18	7:10,12,17	30:25 31:2	188:3,24	133:3
298:25	8:5,20,22	32:21 33:1	189:6	166:3
299:6,11	9:13,18,20	33:9,16	201:15,15	300:4
311:16	160:22	35:17	212:23	<b>better</b> 48:14
319:5,14	162:5	38:17,21	214:6	64:25
323:24,25	173:9	39:18	219:18	154:5
327:21	201:20	46:24	220:9	164:19,24
336:9,13	214:8,10	48:12,21	223:21,23	304:3



**BRIAN J. SCULLY 1/12/2023**

314:13	295:14	212:5	54:10 55:3	179:2
329:21,23	316:2	258:8	55:21 56:3	<b>bucket</b> 44:11
<b>beyond</b> 32:8	337:19	271:13	56:8 70:6	<b>budget</b> 303:9
77:23	<b>biweekly</b>	276:1	70:8,25	336:24
78:12	24:19,19	318:23	71:5,7,11	337:14,18
85:16	31:23	319:1,3	80:14	337:18,22
100:15,16	361:6	<b>Breakdown</b>	128:5	<b>build</b> 16:4
131:13	<b>black</b> 105:17	9:15 346:4	132:5	153:25
136:19	154:16	<b>Brian</b> 1:14	140:1,19	241:9
168:19,24	<b>blanking</b>	2:1 5:2,8	140:22	303:22,25
180:4	103:2	6:3 7:3	141:2	324:10
285:23	<b>blind</b> 308:16	8:3 9:3,15	248:10	332:1
305:10	<b>block</b> 119:25	10:5 11:12	269:24	343:2,20
317:17	<b>blog</b> 82:14	11:18	270:21	358:5
<b>Biden</b> 1:9	82:14,18	158:3	271:3	<b>building</b> 3:8
10:7	114:17	176:3	306:11,13	16:8 46:1
247:22,25	115:7	191:21	307:4,11	131:4
248:14	116:13	200:10	<b>briefings</b>	315:12
375:8	<b>blue</b> 310:3	208:9	27:6 39:23	322:15
376:3	<b>blur</b> 55:10	219:4	49:13	347:19
<b>big</b> 141:8	<b>board</b> 312:22	229:22,24	74:19 81:1	<b>builds</b> 44:5
256:3	<b>bolster</b>	230:12	82:7,8	46:12
269:25	304:16	272:1	238:21	<b>built</b> 348:6
306:13	<b>bots</b> 115:2	283:10	239:8	358:2
<b>bilateral</b>	<b>bottom</b> 83:4	292:25	323:13,14	<b>bullet</b>
36:22 45:4	106:18	372:12	361:10	232:11
239:9,20	109:1	373:8,11	<b>briefly</b>	233:12
241:5,15	111:11	375:12	203:25	243:2
241:18	149:21	376:2	<b>briefs</b> 25:19	262:7
242:16	160:23	377:5,20	159:2	275:18
243:8	173:20	<b>Bridging</b>	<b>bring</b> 28:19	346:10
<b>bio-lab</b>	191:8	366:1	279:13	354:7
323:17	203:15	<b>brief</b> 52:19	<b>bringing</b>	355:9
<b>biolab</b> 324:3	217:4	72:6	304:14	357:1
<b>biolabs</b>	271:23	114:15,17	<b>broad</b> 74:5	<b>bulletin</b>
323:20	288:17	140:2	77:13	365:13,20
<b>biological</b>	356:25	141:9	133:18,23	365:22,24
323:19	<b>box</b> 3:10	248:11	358:9	<b>bulletins</b>
<b>bios</b> 361:6	154:16	361:5	<b>broadening</b>	43:9
<b>bit</b> 14:11	212:22	<b>briefed</b> 70:2	320:4,7	<b>bunch</b> 277:25
26:22 73:5	<b>branch</b> 11:21	70:3 80:24	<b>broader</b> 61:3	<b>burden</b>
102:12	<b>Brand</b> 11:21	137:6	61:4	367:13
143:4	<b>break</b> 35:12	142:18	270:11,15	<b>business</b>
172:25	151:3	362:16	<b>broadly</b>	76:17,19
197:11	172:22	<b>briefing</b>	90:11	76:21
235:17	181:4	21:14	<b>broken</b>	338:16
240:14	183:2	28:18 52:7	258:15	372:19
266:10	189:21	53:14,18	<b>brought</b>	
282:2	192:25	53:20 54:3	17:22	
				<b>C</b>

**LEXITAS LEGAL**

**BRIAN J. SCULLY 1/12/2023**

<b>C</b> 3:1 4:1,1 5:1 6:1 7:1 8:1 9:1 10:1	253:20 255:21 267:24 319:21 325:6 365:14 368:12	333:3,11 333:17,18 333:21 334:8,14 339:13 351:15 352:7 354:12 356:21 358:14 359:23 360:19 361:14	342:22 <b>case</b> 10:8 153:13 158:4 174:10 176:9,12 177:2 188:23 190:10 201:16 210:20,25 211:5,11 217:16 221:9 234:15 257:12 264:11 267:5 340:13 343:16 360:1 366:18 374:11 375:13 376:3	67:13,21 72:20 79:13,16 79:21,25 101:14,21 110:18 112:6 119:9,20 119:24 129:11 141:23 142:4 147:6,18 147:21 149:24 179:8 201:24 262:17 264:15 265:10 267:10,15 267:21,24 278:12 345:24 363:11
<b>C-a-b-l-e</b> 188:7 <b>cable</b> 9:24 188:7 196:17 197:18 198:1 357:9 358:6 359:3 <b>Cable's</b> 195:5 <b>cadence</b> 233:14 234:3 <b>calendar</b> 34:6 274:21 <b>California</b> 2:5 163:10 <b>call</b> 35:11 41:20 85:24 99:9 99:12,15 99:21,25 101:4 103:4 111:22 130:3 282:5 283:3 327:1,4,7 327:9,12 327:12,17 327:20,23 332:18,21 368:11 <b>called</b> 23:16 26:4 48:6 93:10 103:24 112:16 118:7,11 174:13 239:3	<b>calling</b> 348:4 <b>calls</b> 21:8 71:20 72:4 87:17 92:5 92:17 94:15 95:20 96:25 98:11 103:17 108:20 111:8 115:9 118:16 122:22 142:7 149:18 150:19 152:21 153:18 178:15 194:14 198:5 201:4 202:15 204:12,23 231:10 238:11 244:21 257:2 273:1 283:21 294:16,23 294:24 298:11 304:21 310:13 316:19 324:24 332:17,21 332:22	<b>Camargo</b> 186:1 <b>campaign</b> 44:16 <b>campaigns</b> 9:10 127:1 246:20 328:14 <b>capabili...</b> 57:10 108:7 <b>capability</b> 57:14 93:25 94:3 151:13 368:20 <b>capacities</b> 93:15 <b>capacity</b> 57:14,20 76:16 91:19 <b>Capps</b> 3:5 35:10 <b>capstone</b> 321:6 <b>captured</b> 166:4 243:16 <b>carbon</b> 308:16 <b>carefully</b> 13:10 <b>carried</b> 355:10 <b>cascading</b>	<b>Cassandra</b> 1:23 2:2 10:14 374:2,18 <b>catch</b> 91:9 <b>categories</b> 52:22 <b>caught</b> 166:21,23 <b>cause</b> 316:15 317:4 <b>CCR-WA</b> 374:18 <b>CDC</b> 135:12 140:12 322:17,22 323:10 <b>center</b> 11:22 29:7 50:6 52:11 59:7 59:9,16 60:6,17 61:7 62:23 63:19	<b>centers</b> 64:19 112:11 278:5 <b>central</b> 119:24 120:11 157:4 264:15 <b>certain</b> 26:18,24 53:5 61:15 71:12 90:3 104:24 106:16 115:22 137:18 169:17 187:7 199:25 245:1 256:15 261:17 266:3

**LEXITAS LEGAL**

**BRIAN J. SCULLY 1/12/2023**

269:3	206:13	132:12	269:14	208:9,17
274:21	217:4	133:16	285:19	208:25
275:1	223:1,12	150:15	<b>circumst...</b>	210:20,24
348:24	223:16	<b>channel</b>	223:7	211:10,19
363:24	226:6	280:10,23	<b>CIS</b> 59:6	212:8
<b>certainly</b>	282:17	320:25	60:9 61:23	213:17,20
26:21	299:17	<b>channels</b>	62:4,7,12	214:14
67:11	307:1,7	146:23	64:3,17,24	217:5
93:25	<b>chains</b>	<b>chaos</b> 316:15	65:3,11,21	228:3,6,14
129:6	180:25	317:4,5	65:21,22	229:17
182:16	<b>challenges</b>	<b>chapter</b>	66:3,8,15	230:4,24
207:18	317:7	126:14	66:19 67:4	231:2
233:5	<b>challenging</b>	<b>characte...</b>	67:24 68:3	266:2,5
246:10	14:15	121:14	68:7,13,15	267:2
289:12	280:20	300:23	68:19,21	363:11
362:4	302:5,15	318:8	80:11	364:7
<b>certainty</b>	<b>challeng...</b>	347:18	101:24	365:4
75:15	8:18	<b>charge</b>	102:5,6,13	<b>CIS's</b> 210:25
176:10	<b>Chan</b> 7:7	289:12	102:15,24	211:5
<b>CERTIFICATE</b>	29:22	<b>chart</b> 9:23	102:25	<b>CIS-spec...</b>
374:1	237:10	15:9,12	103:1,4,5	112:14
<b>Certified</b>	248:13	18:3 22:12	103:9	<b>CISA</b> 5:18
2:3,4,5,7	249:20	42:21	104:23	8:14,16
4:20	250:4,15	130:9,13	106:10,12	9:12,12
<b>certify</b>	<b>change</b> 28:20	166:17	107:25	11:4 15:9
374:5	127:24	167:4	110:22	15:23 17:6
377:5	128:10	171:22	112:19	17:7 18:25
<b>CFI</b> 45:1	180:7	<b>chat</b> 312:16	119:2	20:17 24:3
<b>CFITF</b> 118:11	286:14	<b>chats</b> 263:14	120:6,21	24:24
118:14	312:25	<b>check</b> 30:20	121:2,6,11	25:25 28:3
120:13	367:2	291:2	121:18	30:14
157:5	376:7,11	<b>checked</b>	148:2,3,12	36:23,24
189:8	376:15,19	70:23	148:18,21	36:25 37:7
198:20	376:23	<b>checker</b>	148:25	37:11,12
199:7	<b>changed</b>	288:2	149:5,9,14	39:15 42:9
217:19,22	127:10,14	<b>checking</b>	157:10,14	44:23
<b>Chad</b> 42:22	271:1	227:5	157:15,17	45:24 46:6
43:18	<b>changes</b>	<b>chief</b> 15:17	157:22	49:5,6
166:17,18	126:24	15:22 28:9	158:15	50:13 51:9
166:24	127:21	289:8	162:21	51:19 52:1
179:18	128:6,16	<b>chose</b> 93:25	165:6,8	53:21
184:13	129:12	<b>chosen</b> 94:2	168:5,13	55:12,13
191:24	133:2,5,9	<b>Christopher</b>	174:23	55:14,17
192:11	134:1,4	191:20	201:24	58:16,20
276:19	284:6	<b>CIA</b> 210:20	202:24	58:21,22
<b>chain</b> 130:6	375:16	<b>circle</b>	203:16	61:8,9,22
157:12	377:7,10	298:24	204:1	62:12 63:6
173:13	<b>changing</b>	<b>circulating</b>	205:4,11	63:16 64:1
175:23	127:6	45:18	205:14,14	64:8,16,19

**BRIAN J. SCULLY 1/12/2023**

65:3 66:2	164:8,11	267:5,17	369:3,6	182:20
66:7,11	164:12	269:20	370:5	199:20
67:6,11	165:22	273:18,21	371:22	218:8,17
70:17 71:6	167:21,22	274:2	<b>CISA's</b> 23:24	262:12
71:11	169:5,25	276:14	25:5 62:16	268:12
72:23	170:6,24	277:25	66:14	278:18
73:25,25	171:17,19	284:13	101:9	325:18
74:4 75:6	172:5	285:1	119:24	335:5
75:13	178:20	290:14	150:15	370:9,17
76:14	183:15,21	302:3,13	151:6,9,9	370:22
77:18	184:1	302:17	188:22	<b>clearing...</b>
79:20	185:16	303:5,6,11	261:13	96:9,17
88:21,23	186:6,15	304:9,16	262:24	<b>clearly</b>
89:5,22	186:25	304:19	264:14	327:8
90:7 94:25	187:9,23	305:3	305:8,17	<b>Clemson</b>
96:9 97:6	188:13	308:1,3	309:5	46:23
97:12,13	189:18,22	310:20	330:18	<b>clips</b> 124:5
97:18 99:1	191:9,14	312:4	342:24	<b>close</b> 131:20
99:14	191:19	313:1,22	347:15,16	131:23
100:11,13	192:18	313:24	<b>citizen</b>	234:5,12
106:3,3,22	195:19,23	314:20	221:15	249:11
108:17,18	196:6,10	315:7	<b>City</b> 3:11	277:3,6
110:17,25	196:19,24	317:10	375:21	331:8
111:5,6,13	197:8,19	318:10,10	<b>civic</b> 200:16	<b>closed</b> 293:8
114:5	198:21	320:10	283:12,16	<b>closely</b>
115:6,13	202:4,4	324:14,21	<b>civil</b> 16:19	289:22
117:20	203:17	325:25	73:11	<b>closer</b> 31:22
118:1	204:9	326:4	105:13	32:4 174:1
119:23	205:15	327:22	109:12,16	174:17
120:1,8,11	207:1,16	330:13	<b>claiming</b>	234:10
122:25	210:7	331:19	280:11	<b>clue</b> 178:17
124:2,13	212:8	332:12,18	<b>clarific...</b>	313:9
124:22	217:19	332:23	218:13	<b>CNN</b> 8:7,7
126:2	218:1,6	333:2,10	219:5	364:15
129:14,20	230:7,12	335:24	223:3,20	<b>coalition</b>
129:24	230:24	336:13	<b>clarify</b> 93:5	97:7,14,16
130:17	232:7,7,25	338:13	132:23	<b>cognitive</b>
133:2,9,19	234:22	345:10,12	229:7	332:7
133:25	238:8	350:20	263:20	338:18,22
134:3	243:8,9	351:1,5	<b>clarifying</b>	339:3
137:19	245:18	352:20,23	83:22	<b>coincide</b>
138:4	248:9	353:16,23	<b>clarity</b>	337:2
142:5,14	251:3	354:8,20	104:2	<b>collaborate</b>
142:21	255:20	355:3,18	<b>clear</b> 66:23	308:3
150:4	256:2	357:1,6,13	66:24	<b>collabor...</b>
151:6	262:16	358:25	104:4,12	111:12,13
154:23	263:2,3,23	360:3,25	130:21	111:18
156:20	264:1,15	365:13	146:22	<b>collabor...</b>
157:4	266:20	368:15	156:3	48:11

**LEXITAS LEGAL**

**BRIAN J. SCULLY 1/12/2023**

52:24	358:11	210:17	77:25	26:1
81:12	371:22	246:11	80:20	154:14
111:17	<b>comes</b> 229:12	255:7	85:20	219:10,16
<b>collabor...</b>	289:18	273:11	87:14	259:6
59:25	367:21	293:14,18	102:6	324:16,23
<b>collabor...</b>	371:17,20	316:23	132:7	325:2
48:24 49:4	<b>comfortable</b>	349:7	133:13,15	329:14
<b>colleague</b>	92:20	<b>Common's</b>	133:17	<b>compound</b>
10:21 71:9	317:24	293:20	147:24	72:3
<b>collected</b>	367:11	<b>commonly</b>	191:12,15	179:21
146:2	<b>coming</b> 64:23	158:13	192:10,20	212:2
<b>collecting</b>	119:13	202:24	277:9,10	226:25
145:24	132:20	<b>communicate</b>	<b>communities</b>	258:6
<b>collection</b>	310:1	18:20	126:19	310:12
156:19	318:18	75:19	259:13	<b>comprehe...</b>
213:14	321:8	168:20	<b>community</b>	295:10
260:1	334:22	326:14	39:20 44:6	<b>computer</b>
<b>collective</b>	358:21	<b>communic...</b>	73:13	152:16
277:25	<b>command</b>	72:1 78:13	84:15	<b>concept</b>
<b>colon</b> 146:4	130:6	245:25	145:21	83:20 99:1
191:9	<b>commence...</b>	247:2	246:19	99:14,18
<b>Colorado</b>	98:17	326:24	257:2	100:14
204:6	362:8	<b>communic...</b>	258:20	<b>concern</b>
205:12,14	<b>comment</b> 92:9	20:7	270:15	42:17
205:22	96:4	<b>communic...</b>	327:14	58:25 65:4
206:5,20	117:24	67:23	332:14,23	66:16
206:21	<b>comments</b>	75:13,24	333:22	67:17
281:19,21	335:16	107:9	334:16,16	126:3
<b>Columbia</b> 2:9	368:8	132:11	<b>communit...</b>	153:4
<b>column</b> 18:6	369:21	134:3	333:1	173:13
<b>combat</b>	<b>Commission</b>	164:20	<b>companies</b>	175:24
333:16	377:24	<b>communic...</b>	17:8,10,13	208:24
<b>combination</b>	<b>committee</b>	66:2,10	109:13	209:2
261:18	307:25	68:4 75:2	241:6	220:2
<b>Combined</b>	352:24	103:9	279:14	250:23
6:22	353:7	106:25	327:14	251:4,12
<b>come</b> 14:13	355:2	136:2	351:3	251:18,22
20:13	359:19,20	146:23	<b>company</b>	352:6,6
44:22 45:5	360:4,25	246:7	155:2	<b>concerned</b>
45:18 84:3	<b>committee's</b>	357:23	<b>complaint</b>	64:22
121:5	361:11	359:9	190:17	271:7
123:11	<b>committees</b>	<b>communic...</b>	<b>complete</b>	286:6
161:9	70:18	20:25 21:3	89:21	288:20
168:5	353:6,11	21:18	373:14	<b>concerning</b>
263:16	353:14	49:10,11	<b>completed</b>	206:20
293:12	<b>common</b> 12:17	49:17,18	365:8	<b>concerns</b>
336:9	158:16	50:1 53:13	<b>component</b>	23:20 24:4
338:9	161:19	53:16 77:7	325:9,11	39:7,13
341:18	162:2	77:13,16	<b>components</b>	58:17 65:9

**BRIAN J. SCULLY 1/12/2023**

66:3 75:4	<b>confirmed</b>	81:7	140:7, 9, 12	<b>contexts</b>
118:25	287:21	108:18	140:14	59:19, 20
124:23	288:1	111:17	<b>containing</b>	<b>contextual</b>
138:6, 10	<b>conflating</b>	<b>considering</b>	225:16	200:15
138:11	147:20	37:23	<b>content</b>	<b>continue</b>
151:8	<b>confronting</b>	226:11	17:18, 20	32:10
161:22	312:23	<b>considers</b>	17:24	63:13
172:17	313:5	320:5	23:22 27:3	210:20
180:17	<b>confused</b>	<b>consisted</b>	27:19	334:3
189:24	13:7	144:17	40:15	<b>continued</b>
204:19	<b>connect</b>	<b>consistent</b>	123:7	170:11
236:14	95:17	122:16	128:10, 16	240:10
240:20	100:18	288:9, 13	129:4, 11	266:5
241:12	<b>connected</b>	306:1	139:12	<b>continues</b>
265:17, 21	50:4, 5, 6	318:3	144:19	213:20
268:5	63:1	344:21	160:5, 11	364:22
291:25	116:23	345:2	160:19	<b>continuing</b>
295:12	140:2	<b>conspiracy</b>	161:10	334:11
338:12	205:23	340:4	177:8	<b>contract</b>
342:2, 5	275:15	<b>conspiring</b>	219:22	331:13
348:14	299:19	286:14	260:9, 13	337:11
366:4, 24	352:11	<b>consult</b>	260:23	<b>contractor</b>
367:23	356:24	34:20	284:7	154:23, 25
<b>conclude</b>	<b>connecting</b>	190:8	288:11	155:1, 13
155:23	100:21	<b>consulta...</b>	289:8, 15	<b>contract...</b>
156:6	101:10	97:6, 12, 13	290:15	331:2, 3
<b>concluded</b>	<b>connection</b>	97:15, 24	295:5, 20	<b>contractors</b>
373:8	98:4 112:5	98:2	296:2	331:7, 11
<b>concludes</b>	124:12	<b>consulted</b>	297:3, 6	<b>contributed</b>
372:11, 11	145:17	98:10	320:17	88:5
<b>concluding</b>	350:16	<b>consulting</b>	<b>contents</b>	<b>contribu...</b>
219:15	<b>connections</b>	97:18	73:6	87:24
<b>conclusion</b>	104:13, 15	<b>contact</b>	163:20	<b>convenience</b>
92:5, 13, 18	104:21	103:5, 16	288:7	307:15
93:12	135:12, 14	103:19, 23	<b>context</b>	<b>conversa...</b>
94:15	<b>connecti...</b>	104:2, 5	20:21	52:4, 5
95:21	264:18	112:14	40:22 41:3	54:14 57:2
156:4	<b>connector</b>	117:18	76:10	58:7, 19
<b>confidence</b>	109:7	157:22	139:16, 18	86:9, 10
27:13, 22	<b>consider</b>	217:5	209:17	98:7 101:1
283:16	45:11	300:5	210:3	117:7
341:19, 24	100:8	350:5, 14	223:16	128:4
342:4, 10	243:19	350:20	274:2	133:20
343:10	332:5	351:2, 7, 24	275:6, 14	135:7, 17
354:24	357:2, 14	<b>contacts</b>	289:1	137:9
<b>confirm</b>	<b>consider...</b>	114:13	309:3	139:13, 21
86:20	123:6	132:1	311:7, 23	139:23
218:23	281:24	135:19	354:17	141:10
219:20	<b>considered</b>	136:13, 23	358:17	142:19

**LEXITAS LEGAL**

**BRIAN J. SCULLY 1/12/2023**

179:9	295:23	117:13	43:12,25	157:10,19
181:20	361:25	119:1	46:11 48:3	157:23
211:13	362:5,7,11	211:18	48:4 50:15	158:7,8,11
254:12	362:13,14	262:9	51:3,6,17	158:12
262:20	362:18	325:6,14	57:23 59:8	159:7,11
267:1	371:20	326:2,6,17	59:23	160:20
268:22	372:3	329:21,24	60:20 63:5	161:6,7
333:1	<b>conveying</b>	332:22	63:18 65:4	162:22,23
348:19	250:23	333:1	65:6 67:1	163:4
371:25	<b>coord</b> 316:13	<b>coordinator</b>	68:6,11	167:3
<b>conversa...</b>	<b>coordinate</b>	216:1	69:23	170:9,17
46:17 47:5	29:2 46:12	<b>copied</b> 67:4	72:17 73:1	170:22
52:15,19	68:13	67:7,11	73:13,18	171:5,16
52:22	74:23	203:22,22	80:15	173:14
64:24 74:8	120:21	213:16	81:13	176:15
74:12,17	130:15	276:24	84:22	180:18
74:22 75:1	212:8	360:2	89:23	182:10
76:2,10,12	214:2	<b>copies</b>	90:19,20	184:12,15
80:17,22	318:5	375:11	91:6,7,17	184:16
81:1,6,8	325:8	<b>Cops</b> 9:4	92:2,15	185:19
81:25 82:4	332:13,20	319:21	93:1,13,16	191:17
82:9 85:25	370:9,18	<b>copy</b> 66:14	93:17	192:4
87:20 98:6	<b>coordinated</b>	67:20	94:12,23	193:10
98:14,16	21:6 30:7	213:20	95:7 96:11	195:12,15
104:9,11	30:11,13	266:14,18	103:10	195:20,24
111:15,19	41:22 42:2	266:22	104:3,18	196:25
112:20,24	42:10,15	308:16	104:19	197:4,8,16
113:2,7,17	69:3 115:1	321:5	105:18	198:21
114:1,9,16	239:5	372:22,24	107:4	199:7,13
114:17	311:10	375:15	108:12	199:14
116:25	<b>coordinates</b>	<b>copying</b>	109:8,14	200:7,11
128:7	46:10	204:1	109:15,23	200:14
133:21,25	<b>coordina...</b>	218:3,5	109:24	203:18
135:10,21	30:16	350:4	110:16	204:3,9
136:4,9	54:20	<b>corner</b>	111:4	205:7,17
139:7,9,11	68:10,19	107:13	112:2,7,8	205:24,25
151:11	68:21 69:5	<b>correct</b>	114:25	206:2,3,8
159:5	121:12	17:24	117:21	206:22
169:1	311:5	19:11,14	118:9	207:22
181:13	317:11,12	19:23	119:3,4	208:12
211:14	317:19	20:10,16	123:10,15	209:18
216:23	329:15	23:1,4,23	125:24	210:4,8,22
237:6,22	332:18	24:14,15	126:19	211:19
238:13,19	<b>coordina...</b>	26:5,6	127:2	212:4
240:17,22	21:8 30:14	29:13	138:12,13	214:21
241:22	36:19,21	30:12	142:5,25	215:17
247:15,17	37:2 47:22	32:15 37:5	149:25	217:6,17
255:5	64:15,18	37:13	150:4,12	217:20,21
259:18	68:4	41:19	150:13	217:24,25

**BRIAN J. SCULLY 1/12/2023**

219:13,24	315:4	4:12 14:6	202:3	322:1,7,10
223:22,23	318:1	34:20 35:4	206:5	<b>COVID-re...</b>
224:3,4,8	326:18	69:10	207:16	322:20
224:12,13	328:3	172:22	212:14	<b>create</b>
224:18,20	329:4,8	374:9	237:23	109:17
225:6	332:15	<b>counselor</b>	238:5	142:3
226:9	335:21,22	308:12	248:23	298:1,3
228:20	336:2	<b>counter</b> 9:9	264:8	317:6
229:10,14	338:13,19	45:2 118:3	268:15	342:1,5,12
229:17	347:8,13	118:6	271:16	363:12,19
233:18,20	352:21,24	254:11	279:3	<b>created</b>
233:25	353:4	328:13	291:16	154:24
234:1	354:25	329:2	303:14	165:22
235:22	355:1,8	332:14	318:17	<b>creates</b>
236:1	361:24	342:24	333:21	56:20
246:16	365:9,18	358:1	351:8	342:25
249:12,13	366:6	<b>countering</b>	<b>course</b> 13:8	<b>creating</b>
250:25	368:24	12:4	13:14	65:11
251:8,8,19	369:4	117:25	128:3	110:1
253:17	370:10,14	118:6	147:19	<b>crisis</b> 325:8
254:1,19	370:15,20	130:1	180:19	<b>critical</b>
254:20,24	371:3	330:14	<b>court</b> 1:1	16:5,9
254:25	373:13	348:12	2:4 3:8	137:24
255:22,23	374:6	<b>counters</b>	10:10 11:8	147:7,15
256:6	377:9,13	331:19,24	12:20 47:9	154:1,5
265:7,15	<b>corrections</b>	<b>counting</b>	153:3	295:10
269:15,21	373:15	337:7,10	190:20	309:6,7
272:6	375:16	<b>countries</b>	<b>courts</b>	322:15,17
280:13,21	<b>correctly</b>	38:3 45:3	355:12	323:6
281:11,24	87:5	45:5,7,18	<b>cover</b> 270:5	327:2,12
282:15	159:20	46:1	<b>coverage</b>	327:13,16
287:15,22	160:13	<b>country</b>	127:20	331:18
288:7,24	189:15	57:13	<b>covering</b>	332:2,4,6
289:24	238:22	<b>County</b> 163:9	174:14	338:17,18
291:12	248:5	228:6,24	<b>COVID</b> 134:11	339:1
292:6,11	270:24	229:12	138:15	340:9,11
292:15	286:12	377:3	140:6,25	340:21,25
293:1,25	306:16	<b>couple</b> 19:18	144:3	341:13,20
295:12	<b>corrects</b>	24:18	263:12	354:21
297:3	167:2	33:13	264:5	355:10
298:17	<b>corrosive</b>	36:16,16	323:10	<b>crossed</b>
299:4,9	344:17	44:3 49:9	324:5	312:13
300:9,10	<b>council</b> 5:15	51:13	<b>COVID-19</b>	<b>Crowd</b> 144:18
300:21	20:5 48:20	56:12	5:13	144:22,23
301:7,9,17	71:8,9,15	77:21	122:12	145:2,13
304:16	71:17,19	81:25	137:22,25	146:7
312:23	136:1,8,14	111:20	138:5	<b>CRR</b> 374:19
314:16,22	336:7	113:2	280:12	<b>CSAC</b> 72:25
314:24	<b>counsel</b> 4:4	197:23	321:25	305:9,11

**LEXITAS LEGAL**



**BRIAN J. SCULLY 1/12/2023**

<b>CSR-HI</b> 374:18	204:22	277:6	367:5,8,17	29:16
<b>CSR-VA</b> 374:18	242:9	281:16,17	<b>decisions</b>	30:11
<b>culprit</b> 323:20	265:18	319:4	49:19	236:18
<b>curb</b> 320:4	266:8	328:20	177:17	248:13
<b>current</b> 11:19	302:20	374:14	178:8	270:20
331:20,25	303:13	377:14	242:4	<b>delibera...</b>
<b>currently</b> 18:24	<b>D</b>	<b>day's</b> 15:1	260:17	156:4
32:11	<b>D</b> 3:3 4:1	<b>days</b> 372:17	<b>declaration</b>	<b>delibera...</b>
160:18	6:1 7:1	372:19	7:4 244:2	155:20
<b>custodians</b> 189:10	8:1 9:1	375:20	244:10	<b>delibera...</b>
191:15,19	10:1	<b>de-dupli...</b>	249:10	152:22,25
276:14,15	<b>D-r-a</b> 186:17	66:4	<b>declare</b>	153:19
276:17,25	<b>D-r-a-z-e-n</b>	211:15	377:12	156:1
277:8	187:17	<b>de-dupli...</b>	<b>decline</b>	<b>delivery</b>
<b>customs</b> 220:10	<b>D.C</b> 3:21	214:2	153:8	373:1
<b>cuts</b> 43:22	375:6	<b>de-dupli...</b>	<b>declined</b>	<b>demo</b> 279:12
<b>cyber</b> 5:19	<b>D/A</b> 316:14	211:17	89:24	279:17
8:11 15:24	<b>D/A</b> 316:14	<b>deal</b> 209:15	<b>declining</b>	<b>Democracy</b>
29:7 76:25	316:17	278:23	51:1	47:8
96:8	<b>danger</b> 304:7	<b>dealing</b>	153:10	<b>democratic</b>
141:23	304:8	162:20	171:6	355:11
235:14,16	<b>dangerous</b>	<b>deals</b> 311:9	<b>deconflate</b>	<b>department</b>
235:24	320:5	<b>dealt</b> 343:13	203:13	3:19 4:13
263:6	344:16	<b>Dear</b> 375:10	<b>dedicated</b>	10:25 11:4
307:22	<b>data</b> 107:14	<b>debunk</b> 220:4	330:18	11:6,23
308:4	107:19	224:7,11	<b>deemed</b> 17:5	44:23
335:19	146:1,1	228:25	<b>deep</b> 274:14	244:12
352:23	<b>date</b> 10:3	290:19	274:24	245:2,17
359:18	86:6 283:5	291:10	<b>DEFENDANT</b>	278:19
360:3,25	345:25	315:3,9	3:16	312:13
<b>cyber-fo...</b> 188:15	373:19	<b>debunking</b>	<b>defendants</b>	316:18,24
<b>Cyberscoop</b> 8:16	376:4	220:22	1:11 4:2	317:2
<b>Cybersec...</b> 4:6	<b>dated</b> 7:4	290:2,14	6:22 10:8	320:3
<b>cycle</b> 47:24	8:19 9:7	315:19	11:1,7	321:8
52:25 56:9	9:10,13,17	<b>debunks</b>	<b>defense</b>	325:5
129:15	248:22	289:24	308:4	337:1
170:8	249:5	<b>December</b>	<b>defer</b> 221:11	343:15
174:19	302:22	248:22	343:14	350:12
185:18	352:21	249:6	<b>define</b> 41:22	351:22
	<b>day</b> 13:13,18	<b>decided</b> 85:8	42:2	375:5
	127:2	116:7	<b>definitely</b>	<b>departme...</b>
	169:8	<b>decision</b>	96:2	278:5,11
	175:3	17:20 22:1	236:10	321:7
	177:3	22:4,5,10	247:16	<b>departme...</b>
	224:5	23:1 164:1	<b>definition</b>	329:1,11
	262:17,22	164:3,16	92:19	<b>departme...</b>
	262:24	178:7	<b>definiti...</b>	92:10
	267:5,21	210:4	133:24	<b>departments</b>
	268:3,5	261:11	<b>Dehmlow</b>	317:8

**LEXITAS LEGAL**

**BRIAN J. SCULLY 1/12/2023**

<b>departure</b>	182:16	308:1	42:3 146:3	77:18,20
36:17	259:17,21	311:15	220:6	78:9
<b>depend</b> 356:5	259:22	312:10	<b>difficult</b>	244:11
<b>depending</b>	336:10,11	320:7	304:9	284:13
28:17	336:19	322:6	<b>difficulty</b>	285:2,13
146:3	351:18	324:16,23	83:17	285:18,24
<b>DEPONENT</b>	372:3	325:8	<b>Digital</b> 47:8	286:5
373:10	<b>detailed</b>	328:12,24	48:21	288:20
<b>deposition</b>	108:11	329:1,7,11	<b>diplomatic</b>	289:22
1:14 2:1	136:7	329:14,20	280:12	290:1,4,6
5:8 6:3	289:3,19	329:23	<b>direct</b> 15:2	291:11
7:3,7 8:3	325:10	369:3,6	15:14	304:9
9:3 10:5	326:6	<b>DHS's</b> 9:6	66:10	305:6
10:12	<b>details</b>	321:5,6	77:25	308:5,13
12:12,16	27:10	<b>DHSA's</b>	79:11	308:13,15
249:20	136:21	319:22	103:8	309:14
372:11	<b>Detection</b>	<b>difference</b>	120:1	310:1,4,11
373:8	107:14	50:3 148:1	147:24	312:15
375:11	<b>determin...</b>	148:7,11	148:22	313:11,14
377:6,8,11	92:20	<b>different</b>	165:9	313:19,23
<b>deputy</b> 12:4	<b>determine</b>	16:18 21:5	173:1	314:11
28:9	44:15	30:5 32:7	367:24	316:11
<b>derived</b>	56:20	38:22 45:4	371:17	335:16
123:3	<b>Detrick</b>	45:6 46:21	<b>directed</b>	336:14
<b>describe</b>	324:2	47:16 49:3	276:14	340:5
41:25	<b>develop</b>	49:25 90:9	<b>Directing</b>	344:6,13
54:25	16:12	91:14	18:2	345:4
59:12 99:9	44:11	108:4	<b>directly</b>	352:21
240:18	131:5	128:22	20:7 27:8	367:19,25
369:8	343:5	155:13	63:24 64:4	<b>director's</b>
<b>described</b>	355:22	161:11	66:6 67:19	313:21
42:23	<b>developed</b>	216:10	110:21	367:20
99:11	43:3	239:16	119:13	368:1
161:20	265:25	242:11	120:7	<b>directors</b>
<b>description</b>	286:16	260:17	135:3	50:10
244:16	<b>developing</b>	262:20	159:7	101:20
345:4	16:17	263:11	161:22	367:19
<b>desired</b>	39:16	264:17	163:3	<b>DiResta</b> 54:5
375:17	333:23	268:19	164:20,23	70:5,20
<b>destroy</b>	<b>development</b>	279:13	266:8	72:17
219:2	172:2	286:13	292:13	116:25
<b>destroyed</b>	187:12,15	291:6	307:2,10	136:9
219:12	<b>developm...</b>	296:20	320:17	139:7,9
<b>destroying</b>	287:19	324:9	<b>director</b>	142:13
218:25	<b>DHS</b> 8:8 9:8	329:13,14	9:13 12:9	361:20
<b>detail</b> 19:19	25:23,24	335:6	22:14,14	368:9
19:22,24	26:1,3	349:6	34:9 76:5	369:22
20:3 71:14	215:13,16	357:22	76:6,7,8	370:3
71:17	220:10	<b>differently</b>	77:8,9,16	<b>dis</b> 5:20

**LEXITAS LEGAL**

**BRIAN J. SCULLY 1/12/2023**

8:14 15:17	351:23	262:7	87:3 90:19	305:25
15:23	<b>discussed</b>	272:22	91:7,18	306:7
19:25	39:9 84:2	274:13	92:3,16	311:8
20:14	86:14	314:18	93:1,21	312:9,14
143:14,18	94:25	318:14	94:13,24	315:4
145:20	114:7	<b>discussions</b>	95:7,11	317:13
150:16	118:21	45:16	96:10,18	319:22
314:14	129:11	52:13	106:14,23	320:8
341:17	131:8	58:15	114:24	322:21
343:6,9	203:12	81:16	118:25	324:8
<b>disclose</b>	216:17	82:21	124:24	326:15
171:6	236:2,8	85:11 95:3	126:23	328:13,25
172:20	238:14	132:21	127:9,12	329:2
<b>disclosed</b>	239:22	137:3	130:16,23	331:17,20
172:19	240:15	150:14	138:10	331:24
192:3	247:5,8	151:5	141:22	332:15
193:2	249:12	178:19	142:4,16	333:15,16
242:15	254:8,23	302:25	147:4	335:20,24
243:7	258:25	305:19,23	149:15,24	336:16
276:16	259:2,16	306:3,6	151:8,23	338:1,7
<b>disclosing</b>	262:11	322:5,11	154:21	340:21,25
150:23	265:12	322:13	160:7	342:24
<b>disclosure</b>	266:20	351:21	169:19	346:12,18
150:19	295:14,23	371:14	172:17	346:22
152:21	306:9	<b>disinfo</b>	180:16	347:6,12
153:18	313:6	282:14,25	182:8	347:21,24
<b>discovery</b>	317:16	285:1,7	189:24	348:14,20
188:22,22	327:6	311:25	193:2	349:7
190:10	333:17	312:4	204:18	354:9,16
191:13	351:1	370:14	220:2	355:4
192:21	356:15	<b>disinfor...</b>	235:25	363:16
193:23	364:2	8:12,18	239:1,10	366:4,24
194:5	<b>discussing</b>	9:6,10,17	240:20	367:23
233:2	13:12	17:5,14,17	242:8	368:20,24
277:3,6	43:10	20:18	261:4	371:3
<b>discuss</b>	109:2	21:22	262:25	<b>disinfor...</b>
39:17	150:11	23:20 24:3	265:16	266:6
82:18	211:9	39:8 40:14	268:5	<b>dismissive</b>
85:18	236:25	41:18,21	278:6,13	335:25
133:2,4,9	237:4	42:1,8,11	283:4	<b>dispute</b>
136:15	305:24	42:13,14	284:13,15	246:14
142:9,13	<b>discussion</b>	42:17	284:15	248:4,6,7
181:10,16	27:18	43:10	285:18	<b>disputed</b>
182:12	78:15	56:15	291:25	223:14
236:18	89:18	57:11,21	300:2	<b>disputes</b>
255:7	171:22	58:17,25	302:4,14	221:15
307:16	236:23	65:4 66:16	302:19	<b>disrupt</b>
308:21	259:8,11	67:5,17	303:6,12	342:20
350:15,21	261:25	75:4 77:3	304:8,19	<b>disrupting</b>

**LEXITAS LEGAL**

**BRIAN J. SCULLY 1/12/2023**

340:14	276:13	152:10	271:5	6:1 7:1,1
<b>dissemin...</b>	277:24	166:10,18	329:3	8:1,1 9:1
246:23	280:5	169:22	<b>domestic...</b>	9:1 10:1,1
<b>distinction</b>	282:2	170:19	279:10	374:2,18
81:11	284:10	173:24	<b>domestics</b>	375:5,10
148:6,13	294:14	174:25	123:9	<b>e-mail</b> 7:8
148:16	295:18,21	181:25	<b>Dominion</b>	7:10 8:20
219:9	305:15	190:12	292:23	9:18,20
<b>distribute</b>	307:6	196:22	<b>downranking</b>	14:13,16
115:5	320:15	197:24	288:6	14:25
<b>District</b> 1:1	321:4,12	211:8	<b>Dr</b> 72:21	66:10,15
1:2 2:8	330:5,7	216:13	<b>draft</b> 9:12	66:25
10:10,10	331:22	222:4	321:4,13	120:7,11
<b>dive</b> 274:14	332:16	226:24	321:17	120:13
274:24	344:5	231:14	352:20	129:3,9
<b>divided</b>	346:7	241:24	<b>drafting</b>	131:18
90:15	348:2	242:2	43:5	157:1,3,5
<b>DIVINE</b> 3:6	354:5	252:9	189:14	157:12
<b>division</b> 1:3	364:17	266:15,21	<b>drafts</b>	161:4,17
10:11 33:2	<b>documents</b>	275:23	321:18	162:11
33:3,15	6:4,13	283:10	<b>dramatic</b>	175:19,23
248:20	7:12,17	289:20	301:2	177:6
<b>DM</b> 281:9	9:5 165:17	290:16	<b>Drazen</b>	179:12
<b>DNI</b> 334:2	176:17	303:19	186:17,21	180:25
<b>DNI-led</b>	294:19	305:12	187:17	193:13
332:21	319:21	313:1	<b>Dropping</b>	198:21
<b>doc</b> 294:9	<b>doing</b> 18:24	324:12	225:20	199:7,19
300:8,12	19:1 40:25	325:2	<b>drops</b> 254:19	201:25
<b>document</b>	41:17	333:24	<b>due</b> 264:4,19	202:13,20
15:8 69:18	43:21 46:2	340:6	<b>duly</b> 11:13	202:22
72:7,11	46:4 47:21	346:4	<b>dump</b> 236:7	203:1,19
98:19	49:14	348:12,13	<b>duplicate</b>	204:4,10
125:2	55:18	349:9,12	64:23	205:6,6
139:6	58:16	355:19	208:10,15	206:13
156:23	68:24 69:2	356:11	208:24	208:13
190:20	74:19,20	370:4	<b>duplication</b>	210:11,16
191:4	87:6,8	<b>DOJ</b> 25:23	120:25	211:6
194:8,11	90:6 106:6	32:16,24	<b>duplicative</b>	213:25
194:13	108:4	33:4,15,19	210:21	214:1,5,19
195:10	120:16	33:25 34:4	212:1	214:24
198:10	121:15,20	117:20	<b>duty</b> 168:23	217:15,20
207:11,12	121:24	248:19	<b>Dynamics</b>	217:22
219:20	127:24	264:18	5:13	223:1,12
244:1,6	128:24	<b>domestic</b>		224:1
249:5	131:10	26:16,23	<hr/>	225:7
250:1	136:12	27:16,20	<b>E</b>	226:11
251:15	139:14	38:4,7,9	<b>E</b> 1:23 2:2	227:18
252:21	140:16	123:13	3:1,1,17	228:11,15
271:15	149:10	270:17,22	4:1,1,1,20	228:22
			5:1,6 6:1	

**BRIAN J. SCULLY 1/12/2023**

230:7, 8, 11	14:5	102:8	367:1, 5	<b>educate</b> 25:1
230:17, 17	188:18	112:23	368:19	239:18
230:24	294:8	115:1	370:6	240:12
237:23	334:25	118:21, 23	<b>earliest</b>	<b>educated</b>
249:14	<b>e-mails</b> 67:5	119:7	22:20, 24	261:5
252:4, 20	67:7	121:11	23:8, 10	<b>education</b>
253:1, 10	131:14	126:9	<b>early</b> 22:7	16:13
253:15	156:19	131:4, 19	22:23, 25	131:5
255:19	166:24	140:9	49:18	239:14
271:25	168:3	147:22	53:14	<b>effectively</b>
277:20	170:20	150:10	63:24 64:6	329:2
278:19	171:4	156:22	70:9 83:24	<b>efficacy</b>
280:16	178:22	157:5, 22	88:25	322:9
281:21	179:13, 17	159:1	89:25 97:5	<b>effort</b> 12:21
282:3, 17	179:23	170:3	173:18	13:5, 10
283:8	180:13, 15	171:21	234:8	203:13
284:24	180:20	174:14	239:25	307:17
285:10	184:7, 11	200:22	240:25, 25	308:2
286:3	184:18	203:12	241:1	320:4
288:18	189:11, 22	208:16	327:2	<b>efforts</b> 8:17
291:9, 20	192:1	246:10	336:12, 13	18:13 96:9
294:2	193:7, 7, 9	255:24	356:7	118:3
296:8	193:21	257:1	362:11, 13	259:14
297:10, 24	201:3	263:7	367:6	302:4, 14
298:24	202:4, 4	264:16	<b>easier</b> 14:20	302:18
299:17, 25	203:17, 23	265:12	144:9	303:1, 1, 6
301:15, 18	213:15	266:20	<b>Easterly</b>	303:7, 11
301:19, 24	215:6	272:20	22:14 76:5	320:8
307:1, 2	230:7	280:5	191:20	321:25
313:10	260:2	284:1	304:10, 13	323:22
317:21	276:24	294:21	305:18	336:4, 6, 20
320:21	277:7	295:24	307:3, 9	<b>EI-ISAC</b>
334:18	278:1	296:1	308:5, 13	60:19
345:14	288:10	301:15	309:14	61:10, 23
350:3, 3, 12	299:19	303:24	310:2, 4, 11	62:1, 2, 5, 7
351:18	340:2	316:5	311:23	110:17, 21
352:2, 4, 17	345:15	320:12	312:15	110:22, 23
356:18	<b>earlier</b>	322:15	313:23	112:10, 13
359:19	20:12 55:2	336:22	314:11	112:18
360:3, 4, 23	56:18, 22	337:24	318:14	147:6, 14
373:4	63:16	340:2	335:16	147:20, 25
<b>E-mail (s)</b>	72:13	351:2	337:24	148:2, 3, 12
6:20	74:14	353:19	344:6, 13	148:21
<b>e-mailed</b>	91:15	355:17, 21	<b>Easterly's</b>	149:13, 20
138:18	93:10	356:3	316:12	199:12
156:12	96:16 98:5	360:12, 24	345:4	204:8
157:15	99:11, 19	362:6	367:25	228:7
194:20	100:16	364:2	<b>ecosystem</b>	<b>eight</b> 196:6
<b>e-mailing</b>	101:17	365:4	357:2, 8	196:10, 12

**BRIAN J. SCULLY 1/12/2023**

233:22	121:18	<b>EIP243</b>	68:4,14	168:21
245:16	122:11	161:15	69:21,22	169:8
250:16	134:11	<b>EIS</b> 67:7	73:3,8,10	170:7,7
<b>EIP</b> 5:9 53:4	136:20	<b>either</b> 75:17	73:16	172:19
54:3 58:14	147:16	104:11	74:21 75:7	174:2,18
59:6 62:12	149:5,9	137:12	78:16,20	174:19
62:24	158:10,14	155:14	79:4,5,7	175:11,12
64:11,13	158:18,19	197:24	79:10,12	179:7,25
64:16,24	162:22	215:13,16	79:17 80:1	180:19
65:4,10,23	169:5	216:22	80:3 83:20	181:11
66:2,7,10	171:15	251:11	83:23	185:17
66:25 67:4	183:21,22	259:21	84:15,24	187:22
67:11,16	184:23	353:6	85:1 87:1	195:18
67:23	185:13	365:24	88:6,13,18	202:14
68:10,21	198:3	368:2	90:10,15	204:18
73:22 74:1	199:11,12	<b>election</b>	90:19	207:7,9
74:4 75:3	199:13,20	5:10,16	91:17,19	208:23
76:12	200:2,11	8:9,17	92:3 93:16	215:12,24
79:10,24	200:19	9:22 16:24	94:23 95:7	216:8,21
80:12,15	201:12	23:25 24:1	95:11 96:6	216:22
81:8,11,18	202:20	24:5,21	96:7,8,16	217:9
82:13 95:1	203:9	25:3,6	97:19	220:7,23
97:25 98:3	208:11,17	26:13	100:18,21	221:4
98:17 99:1	208:25	27:22	101:11,19	228:8
99:12,13	209:15,22	31:21,22	102:10	230:1
99:13,18	210:6,11	31:24 32:4	106:1,4,13	234:6,10
102:7,13	210:19,24	32:5 33:5	107:18	234:13,23
102:15,22	211:4,10	36:11 38:8	110:14	235:12
103:9,13	211:19	38:25 41:8	113:11	239:15
103:21,22	212:7	47:24 48:6	119:23	240:23,24
104:2,7,8	214:2,6	48:9,25	120:3,5,14	241:1
105:2,12	217:16	49:6 50:7	123:2	242:8,11
105:23	228:14	50:10 51:5	126:23,25	244:14
106:5,9,13	229:22	51:20 52:1	127:2,7,15	246:3
106:21	230:1,12	52:12,23	128:11,24	251:17
107:2	230:17	52:25	129:15,24	254:12,13
108:9,12	277:11	54:18,20	130:23	256:15
108:18	362:15,17	54:24	131:6,23	257:20
109:6,18	368:14	55:23 56:4	132:11	258:5,14
109:22	369:7,13	56:8 57:4	134:19	260:11,16
110:2	369:22	57:7,13,19	140:3,22	260:20,24
111:6,7,13	371:15,23	57:25	141:2,3	261:1,2,14
111:14,16	<b>EIP's</b> 66:14	58:24	147:5,5,8	261:19,22
111:18	115:14	59:14 60:1	147:9	262:17,18
112:1,5,21	<b>EIP-243</b>	60:15,23	148:6	262:22,24
116:1,15	158:11	60:25 61:1	149:2,16	264:9
119:2,13	<b>EIP-spec...</b>	61:5 62:20	163:22,24	265:10,18
119:14	169:14	63:12,24	164:4,20	265:21
121:12,15	200:7	64:1 67:10	165:9,10	266:1,7,8

**LEXITAS LEGAL**

**BRIAN J. SCULLY 1/12/2023**

267:4,12	126:4	<b>employment</b>	305:7	204:17
267:13,21	127:8	196:24	318:12	324:3
268:1,3,5	132:14,19	<b>enable</b> 73:9	347:1,4,7	369:15
269:25	304:19	<b>enclosed</b>	347:9,13	<b>entry</b> 98:23
270:5,8,15	332:15	375:11,13	348:1	290:9
280:2	355:3	<b>Enclosures</b>	<b>engagements</b>	<b>environment</b>
282:14,25	<b>election...</b>	375:25	18:7,10	48:15
283:4,16	304:5	<b>encouraged</b>	19:9 44:22	152:1
285:20	<b>elections</b>	318:5	45:4 298:8	154:6
286:21	8:4 25:2,8	<b>encouraging</b>	299:1	<b>Erie</b> 217:10
297:5,12	27:14	128:9	<b>engages</b>	<b>errata</b>
297:22	48:15	<b>ended</b> 49:15	171:3	373:16
298:1,10	215:10	51:16	<b>engaging</b>	375:14,17
298:16	216:1	65:18,25	18:10	375:19
300:20,24	234:4,5	195:14	73:17	376:1
301:8	239:14,18	336:11	78:20 79:4	<b>erry</b> 281:16
302:4,14	240:13	337:21	286:21	<b>escalate</b>
302:18,19	263:5	<b>ends</b> 19:17	329:14	176:3
303:12,13	269:20	<b>enemies</b>	346:21	206:2
304:16	270:11	285:22	<b>ensure</b>	207:25
305:6,7	296:17	<b>enforcement</b>	253:23	208:2,11
306:15	299:2	95:13	<b>entailed</b>	226:15
307:5,12	308:23	220:11	169:13	292:25
315:15	315:16	245:25	<b>enter</b> 165:25	297:3
332:24	331:17	250:5,17	166:7	<b>escalated</b>
336:1	332:12	250:21,22	<b>entire</b>	200:11
339:4,6	334:4	251:2	174:19	<b>escalating</b>
340:14,16	340:14	320:21	180:19	158:5
340:18	364:8	366:6,9,14	194:8	295:5,20
344:18	<b>Ellis</b> 1:23	<b>enforcing</b>	195:23	<b>ESI</b> 276:17
354:23,24	2:2 4:20	289:15	219:13	276:25
360:10	10:15,15	<b>engage</b> 16:18	357:7	<b>especially</b>
362:1,8	374:2,18	184:18	<b>entirely</b>	95:11
363:12,14	<b>Elvis</b> 7:6	266:1	29:8 77:1	164:23
363:19	29:22 30:1	322:17	101:20	<b>ESQUIRE</b> 3:3
364:20	237:10	346:12,17	188:11,16	3:4,5,6,17
365:1	248:13	347:24	261:17	3:18 4:3
366:1,12	249:20	<b>engaged</b>	295:24	4:11 375:5
366:17	<b>emerging</b>	44:25	363:22	<b>essential</b>
368:9,24	109:21	73:21	<b>entities</b>	128:6
370:14	<b>emphasize</b>	130:18	46:21 48:2	267:16
371:2	372:8	<b>engagement</b>	109:13	<b>essentially</b>
372:1	<b>employed</b>	18:13,15	<b>entitled</b>	17:3 18:12
<b>election...</b>	374:10	43:19 44:4	233:13	19:9 28:8
262:9	<b>employee</b>	46:7 82:2	244:2	40:17
264:22	120:2	146:1	277:4	41:11
265:9	278:20	172:2,4	302:3	43:17
<b>election...</b>	<b>employees</b>	187:15	328:12	45:13 47:2
125:23	337:9	278:5,11	<b>entity</b>	54:11,14

**BRIAN J. SCULLY 1/12/2023**

57:12	331:9	73:22	252:15,18	19:21
59:12 62:9	<b>exactly</b>	292:21	255:15	259:3,4
67:24 85:4	15:21	<b>exchanges</b>	259:24	<b>expectation</b>
86:19	68:24 93:5	250:3	269:4	175:4,19
117:15	101:21	<b>excluded</b>	277:16,19	193:16
154:2,7,12	137:15	95:13	301:20	261:9
155:19	152:15,19	<b>Exclusive</b>	302:1	<b>expectat...</b>
263:2	221:9	8:8	306:18,20	247:7
291:2	275:25	<b>excuse</b> 82:14	309:20,23	<b>expected</b>
294:2	307:21	313:17	319:15,18	246:1,19
305:4	337:12,20	350:3	328:4,7	<b>expecting</b>
323:17	<b>EXAMINATION</b>	<b>executed</b>	334:19,25	179:10
348:18	5:2 11:14	249:11	335:1,6,12	<b>expedited</b>
358:20	<b>examined</b>	377:14	345:18,20	6:24
<b>establish</b>	373:12	<b>executive</b>	349:15,18	372:17
126:18	<b>example</b> 28:7	73:6 89:15	349:24	<b>experience</b>
<b>established</b>	43:2 44:13	<b>exhibit</b> 5:8	350:2	318:4
55:24	58:16 66:9	5:9,11,14	352:13,16	<b>expert</b>
215:24	78:6	5:18 6:3,4	359:13,16	108:11
313:2	103:12	6:13,20,22	363:6,9	361:20
364:5	147:3	7:3,4,6,8	364:11,14	<b>expertise</b>
<b>et</b> 1:6,10	161:12	7:10,12,17	365:10,13	25:6,8
10:6,7	177:2	8:3,4,7,11	368:3,6	343:18
375:8,8	189:10	8:14,16,20	369:17,20	<b>experts</b>
376:3,3	221:14	8:22 9:3,4	369:23	337:25
<b>evaluate</b>	223:3,24	9:8,12,15	<b>exhibits</b>	338:7,10
23:21	240:4	9:18,20,22	188:19	343:14,21
<b>evening</b>	243:8	9:24 13:25	212:14	356:4
226:7,23	263:16	14:4,4,6,7	237:24	361:5,10
226:24	292:4	69:7,9	252:14,16	361:16
227:4	315:18	138:17,20	277:25	<b>Expires</b>
<b>event</b> 5:14	332:10	156:13,14	301:25	377:24
5:18 78:3	336:21	168:4	318:18	<b>explain</b>
117:4	339:24	170:20	345:14	151:21
332:3	340:3,16	173:2	<b>exist</b> 166:5	153:14
<b>events</b>	341:23	179:13	<b>existed</b> 98:8	223:12
331:21,25	342:25	190:13,16	<b>existing</b>	342:3
<b>everybody</b>	357:15	194:19,25	283:13	<b>explained</b>
65:20	<b>examples</b>	197:25	<b>expand</b>	71:3
211:22,23	126:10	198:10	300:18	<b>explanation</b>
211:24	158:11	212:25	302:18	221:19
<b>evidence</b>	265:2	213:14	<b>expanding</b>	229:13,17
219:2	<b>excellence</b>	227:9,12	151:6,9	<b>explicit</b>
<b>exact</b> 85:4	141:23	231:15	301:1	90:18 91:5
86:5	142:4	242:12	303:6	94:22 95:6
129:23	149:24	243:22,25	320:10	<b>extensive</b>
134:24	<b>Excerpts</b> 7:6	249:15,17	<b>expands</b> 8:17	152:3,3
190:2	<b>exchange</b>	249:22	302:3,14	<b>extent</b> 53:16
307:24	73:10,17	252:3,5,12	<b>expect</b> 19:15	79:24 92:5

**LEXITAS LEGAL**



**BRIAN J. SCULLY 1/12/2023**

94:15	225:5,11	102:9,12	<b>false</b> 207:9	216:16
100:19	225:16	102:14,18	219:11,17	244:13
121:22	233:23	103:12	224:2	245:6,18
124:17	241:6	104:22	283:14	248:12,13
136:21	243:9	327:12	288:3	250:17,24
137:8	253:15,23	<b>facilita...</b>	<b>falsely</b>	251:4
141:5	255:20,25	111:25	280:11	264:18
150:19,22	256:2	<b>facilities</b>	354:24	270:17
153:17,21	271:24	342:19	<b>familiar</b>	316:2
158:20	272:24	<b>fact</b> 43:1	15:12,13	366:18
184:7	275:4	55:11	69:17	<b>FBI's</b> 271:6
287:20	284:12,25	76:13 87:9	77:23,24	<b>FBI.gov</b>
364:3,4,6	284:25	124:16	85:19	215:2
365:6	286:4	154:20	107:1	<b>FBI/CISA</b>
<b>external</b>	287:4,12	197:22	123:19,21	206:21
108:15,18	287:17	207:6	131:9	<b>February</b>
109:2,4,11	293:15	219:1	239:15	327:25,25
133:8,11	294:7	234:3	266:11	328:2
329:21,24	295:18	235:15	279:25	350:8
369:8,15	296:6	238:4	328:16,18	<b>FEC</b> 244:2
<b>extraord...</b>	297:6	242:7	335:2	<b>FED</b> 314:13
35:7	307:2,3,10	276:22	364:23	<b>federal</b>
<b>extremely</b>	307:12,14	277:3	365:19	16:20 21:5
192:7	308:6	288:2	<b>familiarity</b>	25:11
<b>eyesight</b>	309:14	291:2,9	182:18	31:15 37:1
297:17	310:6,21	309:15	<b>far</b> 14:14	37:12 44:7
	310:25	348:11	17:25	55:23 56:5
<b>F</b>	311:2	<b>factors</b>	107:6,8	91:16 92:1
<b>face</b> 308:25	320:18,20	339:2	112:17	92:14,25
<b>Facebook</b>	348:15	<b>facts</b> 344:15	125:1	93:19,24
21:7 27:3	<b>Facebook...</b>	344:17,24	138:13	94:6,11,17
36:23,24	144:24	345:11	172:14	96:24
37:4,11	<b>Facebook...</b>	<b>fair</b> 13:23	182:23	128:9
38:15 65:3	159:13	13:24	234:3	136:24
78:7 117:3	<b>Facebook...</b>	298:15	334:13	149:25
117:10,12	320:24	329:17	<b>fast</b> 12:22	150:4
117:16,19	<b>faced</b> 83:23	345:5	275:22	178:11
127:6	<b>facilitate</b>	369:13	<b>FBI</b> 25:23	235:2
146:6	25:16	<b>fairly</b> 36:9	29:10,14	245:24
159:7,17	59:25	57:8	29:19 30:6	246:12
159:18,22	74:22	114:15,16	30:15	250:4,16
176:15	103:16	<b>fall</b> 51:17	117:20	250:21,22
217:24	210:21	51:19	207:1,16	258:3,11
218:2,7,10	220:19	170:14	214:19,20	264:5,12
218:10,12	263:4	184:4	214:20,21	267:6,8,19
218:19,23	264:10	186:8,10	215:1,8,13	286:14,20
219:4,23	<b>facilitated</b>	187:6	215:16,18	315:9
220:9	50:10	315:18	215:22,25	317:2,12
221:16	52:10	359:10	216:4,5,11	337:9

**BRIAN J. SCULLY 1/12/2023**

370:9,12	341:11,22	202:5	67:17	308:7
370:18,25	341:25,25	213:13	180:16	352:2
371:18	342:4,11	224:1	207:21	<b>follow-up</b>
<b>feed</b> 155:8	343:1,4,11	228:17	291:17,18	13:19
<b>feedback</b>	343:13,18	233:11,11	295:5	116:8
88:14,17	343:22,24	253:5	<b>Fleischman</b>	<b>followers</b>
294:11	355:13,16	260:3	4:11 11:4	206:8,17
361:17	355:20,23	277:5	<b>flexibility</b>	207:22
<b>feel</b> 167:17	356:4,5,13	278:2	330:15	<b>following</b>
<b>fellow</b> 89:4	374:11	299:11,13	<b>flip</b> 117:22	65:18
<b>felt</b> 16:10	<b>find</b> 62:20	299:15,23	<b>flipping</b>	89:16
235:4	108:25	310:5	109:10	115:6,13
<b>field</b> 215:23	143:14,17	319:9	<b>floor</b> 267:24	115:17
215:25	179:23	320:2	<b>flows</b> 105:17	191:14
216:5	180:7	335:23	106:19	199:12
<b>fifth</b> 101:4	220:24	345:15	110:22	203:7
195:9	221:13,24	354:7	357:20,22	253:24
<b>fight</b> 8:17	222:3	356:11	<b>focus</b> 13:22	290:13
302:4,14	224:11	360:4	59:1	291:1
302:18	315:8	370:22	330:15	<b>follows</b>
303:6,12	329:5	371:16,20	354:8,20	11:13
303:20	375:11	<b>five</b> 38:25	355:3	299:24
304:14,18	<b>finding</b>	180:12	357:19,25	<b>force</b> 12:5
<b>figure</b> 49:20	367:3	181:1	<b>focuses</b>	118:1,7
86:6	<b>findings</b>	192:11	331:16	130:2
102:19	47:6	201:1	<b>focussed</b>	271:6
221:17	<b>finds</b> 298:24	243:2	61:1	312:3
275:12	350:12	276:18	<b>foggy</b> 22:19	330:15
<b>figuring</b>	<b>finish</b> 113:3	282:5	101:6	348:13
274:4	<b>first</b> 6:24	319:3	<b>Foley</b> 71:10	<b>foregoing</b>
<b>file</b> 116:1	12:15,16	330:25	<b>folks</b> 29:17	373:12
<b>filed</b> 190:19	12:19 14:7	<b>fix</b> 83:6	46:22 52:6	374:4,5
244:1	24:12	<b>flag</b> 109:21	52:11	377:6,13
<b>filing</b>	25:21	110:1	58:11 70:2	<b>foreign</b> 12:5
375:21	31:14	192:2	70:3 83:23	26:15,21
<b>fill</b> 58:1,16	55:16	251:18,18	85:5,20	39:21 41:9
58:22	56:25 78:6	281:3	104:5,23	45:2,9,9
315:22	81:25	297:3	147:20	45:14,18
<b>filling</b>	95:14	320:17	165:18	117:25
58:20 85:1	103:2	364:20	188:25	118:7
<b>filter</b> 62:4	109:11	365:1	234:18,20	122:13
<b>final</b> 194:10	117:15	<b>flagged</b>	264:9	123:3,9,13
194:12	125:21	116:12	267:13	130:1
243:13	144:11	177:9	327:15	256:20
299:8	153:5	206:6	<b>follow</b>	259:13
<b>finalized</b>	156:25	288:12	137:21	271:6
321:22	157:17,18	292:22	197:22	323:18,22
<b>financial</b>	185:25	<b>flagging</b>	287:24,25	329:3
340:23	187:18	21:21	289:3	330:14

**LEXITAS LEGAL**

**BRIAN J. SCULLY 1/12/2023**

348:13	159:16,21	<b>forwards</b>	269:19	193:4,6
364:18	168:6,10	205:5	276:23	265:5
<b>Forensic</b>	175:14,18	217:22	<b>fourth</b> 44:11	270:12
48:22	175:24	<b>found</b> 153:3	90:5	<b>functioning</b>
<b>forget</b> 29:17	205:16	328:23	185:22	341:21
54:7 102:1	216:16	<b>foundation</b>	249:5	<b>functions</b>
116:22,23	217:23	39:2 80:5	251:16	304:4
155:13	220:2	122:22	321:3	354:21
174:4	231:1	145:11	364:16	355:10
186:1	259:9	149:18	<b>frame</b> 99:17	<b>fund</b> 110:23
214:4	280:25	178:15	220:5	<b>funded</b> 61:8
286:16	281:23	196:1	<b>framework</b>	89:21
307:23	336:25	197:2	44:14	<b>funding</b>
<b>forgetting</b>	<b>forwarded</b>	204:24	<b>Frameworks</b>	61:10,12
167:18	17:21 24:3	214:23	47:8	61:23 62:1
<b>forgot</b> 30:1	119:11	233:25	<b>framing</b> 42:7	149:1,2
<b>form</b> 116:17	131:14	244:21	<b>fraud</b> 341:17	303:9
148:8	135:4	245:8,12	<b>frequency</b>	368:21
228:18	137:13	304:21	31:19	<b>funds</b> 110:18
347:1,4	159:7	313:8	<b>frequent</b>	337:17
359:5	178:4	333:19	31:20	<b>funky</b> 299:18
377:7	180:20	350:24	<b>frequently</b>	<b>further</b>
<b>formal</b>	184:8	353:25	39:4 64:4	31:20
234:16	189:23	354:13	<b>Friday</b>	102:6
<b>formalized</b>	193:2	355:6	291:17,20	221:17
142:15	200:19,20	356:22	291:21	307:16
320:16	206:16	359:23	292:1,6	318:14
<b>formally</b>	207:24	361:14	293:17	332:9
276:12	218:1,18	<b>foundati...</b>	304:10	347:10
<b>formation</b>	226:7	304:3	<b>front</b> 187:2	<b>fuse</b> 5:9
318:20	229:16	<b>four</b> 12:1	328:8	141:3
<b>formed</b> 58:12	281:12,15	19:8 31:18	<b>frozen</b> 82:24	<b>future</b>
73:9	281:22	35:24	82:25	367:15,19
<b>former</b>	366:20	48:13,13	<b>full</b> 11:17	367:21
304:15	<b>forwarding</b>	48:16,17	69:4 80:9	368:1
<b>forming</b>	23:25 67:8	48:24	261:8	<b>fuzzy</b> 81:11
100:8,10	67:9	89:20 90:1	264:3	<b>FYI</b> 199:20
<b>Fort</b> 324:2	134:25	105:12	342:20	<b>FYSA</b> 199:11
<b>forth</b> 27:4	175:6,20	110:7	<b>full-time</b>	
127:6	179:25	111:11	170:10	<hr/> <b>G</b> <hr/>
144:20	183:15	112:22	330:19,25	<b>G</b> 10:1
370:19	184:11	113:24,25	<b>fully</b> 148:16	<b>G-e-o-f-f</b>
<b>forum</b> 45:2	192:1	141:16,17	<b>fun</b> 291:21	308:18
<b>forward</b> 13:3	202:24	184:22	<b>function</b>	<b>G7</b> 44:25
13:13 17:6	205:11	185:12	25:2 63:17	45:12
63:25	217:7	192:11,25	63:20	<b>GAC</b> 316:5
106:12	242:10	214:21	161:20	<b>Gadde</b> 360:14
123:5	278:4,6	250:8,12	163:18	360:14
129:8	291:24	256:4	189:23	<b>gaining</b>

**LEXITAS LEGAL**

**BRIAN J. SCULLY 1/12/2023**

229:4	108:20	231:10,18	371:10	25:14,15
<b>gap</b> 49:21	111:8	231:21	372:7,20	27:7,10,17
52:6 56:24	115:9,15	242:18,22	372:21,23	29:20
57:1,12,17	115:20	244:20	373:2,5	33:21 36:6
57:18 58:2	116:17	245:7	375:5,10	37:8,19,21
58:16,20	118:16	249:16,19	<b>gateway</b>	38:10,16
58:23	122:21	252:7,11	123:19,23	38:19 41:4
74:18	125:6,9	252:19,24	124:23	41:21,22
83:22 84:4	126:5	253:2,4,7	125:18,22	44:21
84:6,8,9	130:19	253:12	126:3	52:21 57:5
84:11 85:2	138:22	255:16	<b>gathered</b>	59:1 64:7
85:5,21	139:2	258:6	107:19	65:5 67:20
86:14,21	142:6	262:2	<b>gathering</b>	68:13 74:2
86:22 87:1	145:3,6,10	271:10,17	107:15	79:19
87:9 91:14	146:16	273:1	<b>GEC</b> 111:3	80:18,19
91:16,18	148:8	276:3	280:1	80:23
92:1,14,23	149:17	277:13,21	<b>Gegovich</b>	83:18 94:4
93:8,10,15	150:18	283:21	141:13	107:5,7
93:18 94:5	152:20	294:16,23	<b>general</b> 4:12	119:7,13
94:10,17	153:7,17	298:11	21:2 32:22	128:2,7,22
96:15,23	155:25	302:6,10	39:14	143:12
98:7 99:10	156:8	304:20	49:22 60:3	153:14
111:22	161:25	306:21	62:16	163:21
368:19	178:14	310:12	124:14,16	176:23
370:5,12	179:21	313:7	133:1	177:16
<b>gaps</b> 57:6	181:2,8	316:19	141:6	178:18
96:23	183:3,10	318:21	145:20	193:18,19
315:22	185:7	319:8	235:7	212:11
372:1	190:21,24	324:24	238:12	215:11,22
<b>Garcia-C...</b>	194:14,21	333:18	240:17	220:14
186:3	195:25	334:20	247:15	222:5
<b>Gardner</b> 3:17	196:4	335:1,4,8	266:13	233:14
10:24,25	197:1	339:13,19	268:14,22	234:2,23
14:12,19	198:5,22	341:6	328:12	235:7
23:2,5	199:3	344:7,10	330:16	239:23
34:15,18	201:4	344:25	346:19	257:6
35:4 53:1	202:15	345:6	348:19	258:21
69:11	204:12,20	349:25	358:17	263:10,12
71:20 72:3	204:23	350:23	371:19	264:25
77:10,19	212:2,17	351:15	<b>General's</b>	278:17
80:4 87:16	212:21,23	352:7	3:7 10:20	288:13
90:25 92:4	213:6	353:24	10:23	293:19,22
92:17 93:2	214:22	354:12	35:10	304:2
93:22	215:3	355:5	<b>generality</b>	309:4
94:14	226:25	356:21	153:22	315:23
95:20,24	227:14,19	358:14	154:10	325:19
96:25	227:22	359:5,22	<b>generally</b>	333:5,6,22
97:20	228:18	360:19	15:21 16:7	340:10
98:11	230:19	361:13	24:24 25:7	343:14

**LEXITAS LEGAL**

**BRIAN J. SCULLY 1/12/2023**

349:5	13:1 40:3	197:25	200:13	238:18
357:18,19	50:17,19	198:9	210:1	249:14
359:7,11	87:5	209:4,6	242:21	254:4
366:16	136:17	210:1	254:15	259:9,24
369:8	190:1	215:21	299:6	262:4,21
<b>generate</b>	210:8	217:2	304:12	263:5
159:24	214:16	218:14,15	312:21	270:4
<b>generic</b>	282:6	221:3,7,23	338:15	271:11,16
100:6	283:11	222:10	357:5	277:4
<b>generically</b>	284:2,5,6	231:22	369:1	288:16
155:6	339:24	241:10	<b>going</b> 14:9	290:11
358:7	345:23	253:4	14:11 15:1	296:18
<b>gentleman</b>	346:1	256:24	20:4 21:16	298:20
310:6	<b>given</b> 12:12	257:10	27:2 31:12	301:24
<b>Geoff</b> 22:11	373:14	266:25	32:13	302:19
25:14,25	<b>gives</b> 272:4	271:10	39:22	307:20
28:4,10	<b>giving</b> 27:6	273:8	48:14	334:9,15
53:23 54:1	55:20	274:20	50:17,19	334:24
75:25 76:2	270:20	275:2,22	50:24	336:15
130:5,5	<b>Gleicher</b>	276:11	54:16 56:1	358:3
191:21	310:17,18	277:19	77:24	<b>good</b> 29:24
253:17	311:22	279:15,16	89:14	56:14,21
270:2,3	312:16	288:5	102:20	66:20
308:18,19	<b>global</b> 278:5	289:24	122:2,5	109:1
309:17	278:11	294:4	125:1	134:13
333:5	<b>globally</b>	302:10	138:16	140:11
350:4	236:21	315:8	140:5,24	163:6
353:20	255:8	330:4	144:6	181:4
360:23	273:11	332:9	156:10	247:14
<b>George</b>	<b>go</b> 12:17	333:13	162:8,12	271:12
279:20,22	13:3 15:1	342:14	166:20	276:3
<b>Georgetown</b>	34:22	348:6,17	167:11	279:6,10
46:24	53:12	349:6	172:20	282:4
<b>getting</b>	61:16 83:2	350:2	173:9	284:23,25
40:18	83:5,5,7	362:20	179:3	286:5
100:2	88:22	364:16	181:3	330:6
102:18	113:3	365:16	183:24	331:12
109:4	120:17	370:1	184:2	341:23
125:10	124:8	<b>goal</b> 54:22	193:13	346:16
203:22	125:6	347:19	198:23	<b>Google</b> 38:16
208:16	127:13	<b>goes</b> 13:13	208:4	144:18
220:19	152:17	19:12 62:2	209:20	233:23
228:9	165:17	62:3,3	211:10	350:5,16
293:4	182:21	90:16	212:14	<b>Google-s...</b>
299:8	183:4	94:19	218:15	161:5
344:1	186:10	95:10	220:11	<b>Gotcha</b> 79:22
345:14	188:4	109:20	229:2	126:15
<b>gist</b> 54:14	191:3	110:21	230:24	141:18
<b>give</b> 12:24	195:4	158:9	233:7	218:11

**LEXITAS LEGAL**

**BRIAN J. SCULLY 1/12/2023**

gov@twit...	318:6	325:16	9:1	312:4
300:5	320:17,20	326:3,6,13	<b>H-i-c-k-e-y</b>	<b>handle</b> 215:5
<b>governance</b>	320:25	326:16,17	33:17	265:1
312:22	348:22,23	359:19	<b>hack</b> 236:6,7	281:8
<b>government</b>	348:25	368:15	236:14,18	<b>handling</b>
9:16 21:4	369:2	<b>groups</b> 16:19	237:4,14	31:5 312:5
24:14 28:1	370:13	38:12 46:8	246:1,13	<b>happen</b> 62:15
38:6 40:4	371:1,18	47:10,13	247:7,21	219:25
40:13 41:2	372:7	50:7 110:8	250:18,24	241:15
44:7 45:14	<b>governme...</b>	111:12	251:12,22	256:15
45:14	94:6,11,17	349:7	254:17,22	315:21
55:23 61:3	109:25	<b>grow</b> 336:15	255:2,11	351:4
73:10,16	178:23	336:20	255:11	<b>happened</b>
73:20 75:3	194:5	<b>guess</b> 19:8	274:9	100:25
78:6 90:16	257:25	66:1 76:6	275:6,13	101:7
90:17 91:4	339:7	104:25	275:15,19	106:22
91:16 92:2	<b>governments</b>	111:17	<b>hack/leak</b>	139:23
92:25	45:9	203:5	272:10,17	168:17
93:20,24	105:22	227:4	274:24	210:10
94:21 95:5	323:18	269:3	<b>hacker</b>	229:8
105:13,16	369:4	290:10	274:11	246:15
105:17,21	<b>graduated</b>	307:11	<b>hacking</b>	265:8
106:20	172:14	348:12	246:21,22	268:11,17
109:12,16	182:25	<b>guidance</b>	<b>Hale</b> 22:12	293:19
110:5	<b>grant</b> 61:14	22:14	25:14,25	301:14
117:14	<b>grants</b> 61:12	216:21	28:4 53:23	337:20
127:23,24	<b>graphic</b> 43:2	358:18	54:1 75:25	351:8
128:9	105:12	<b>guy</b> 263:16	191:21	<b>happening</b>
132:5	107:13	<b>guys</b> 63:9	253:17	117:1
135:4	108:8	173:23	270:2	253:9
137:13	110:8	179:16	308:19	268:22
140:14	330:9	185:7	309:17	<b>happens</b>
142:3	<b>Graphika</b>	216:13	350:5	36:22
146:24	47:13 48:3	226:23	353:20	176:13
149:25	48:19	249:21	360:23	264:21
150:4	<b>grateful</b>	264:24	<b>half</b> 271:23	279:9
153:2	294:10	265:4	273:15	323:18
156:20	<b>gray</b> 310:5	303:19	<b>hammer</b> 286:6	347:17
179:10	<b>great</b> 295:3	344:8	286:11	<b>happy</b> 14:24
221:19	<b>ground</b> 12:18	366:8	288:2,21	307:14
236:25	<b>grounds</b>	<b>Gwinnet</b>	340:3,7	312:16
244:18	152:21	228:6	<b>hammer/s...</b>	<b>harassment</b>
257:7,17	155:25	<b>Gwinnett</b>	289:21	8:9 50:24
257:22,23	<b>group</b> 47:14	228:24	291:10	<b>hard</b> 27:7
258:1	76:23 89:6	229:12	<b>Hampshire</b>	86:6
275:8,12	111:7		299:12,22	177:11
286:20	197:12	<b>H</b>	<b>hand</b> 374:14	178:7
314:2,10	233:8	<b>H</b> 5:6 6:1	<b>handing</b>	180:2
317:24	325:7,14	7:1 8:1	174:5	293:18

**BRIAN J. SCULLY 1/12/2023**

305:16	<b>height</b> 331:6	139:13	253:9	141:23
337:6, 11	331:10, 12	179:2	277:21	142:4
359:25	<b>heightened</b>	208:9	302:8, 8	149:24
<b>harder</b>	126:22	224:6	344:7	150:3
340:18	<b>held</b> 2:1	226:19	<b>holiday</b>	<b>HSH</b> 322:23
<b>harms</b> 342:12	10:12	257:17	373:6	<b>human</b> 28:21
342:13, 15	<b>help</b> 16:14	259:2	<b>Homeland</b>	34:9
<b>Harvard</b>	44:14, 17	<b>HHS</b> 135:12	4:13 11:5	340:15
46:22	100:20	140:12	11:23	<b>hundred</b>
<b>Hawaii</b> 2:3	131:6	322:18	244:13	26:18
<b>head</b> 12:25	210:4	323:10	245:3, 17	137:17
13:3 130:1	216:8	<b>Hi</b> 161:4	320:3	169:16
241:20	220:4	228:7	321:5, 13	<b>Hunter</b>
<b>headed</b>	260:19	283:10	321:15	247:21, 24
117:12	261:22	350:11	<b>hone</b> 359:8	248:14
<b>header</b>	307:17	<b>Hickey</b> 33:12	359:11	<b>hyper</b> 357:10
199:24	316:8	<b>high</b> 3:9	<b>honest</b> 65:17	358:12
205:18	322:16, 18	153:22	91:21	359:3
226:11	323:5	154:9	113:20	<b>hypothet...</b>
282:23	324:10	337:3	135:2	339:14, 21
297:23	343:5	<b>high-level</b>	148:15	343:25
<b>header's</b>	355:23	25:18	177:24	<b>hypothet...</b>
297:16	356:6	27:11 40:5	216:14	339:16
<b>heading</b>	358:18	257:3	259:19	344:2
122:10	<b>helpful</b>	<b>higher</b> 37:22	261:16	
<b>headline</b>	155:21, 24	130:12	322:25	<b>I</b>
302:13	162:12	296:5	<b>honestly</b>	<b>I-S-A-C</b>
319:25	299:3	<b>highlight</b>	22:17 29:6	59:21
<b>heads</b> 210:8	300:9, 12	305:16	54:7	<b>I&amp;A</b> 26:8
284:3, 5, 6	<b>helpfully</b>	346:9	124:20	27:8 28:14
311:15	220:24	<b>highlighted</b>	176:18	28:22
<b>health</b>	<b>helping</b>	150:5	303:18	264:18
136:24	58:22, 23	<b>highligh...</b>	<b>hope</b> 158:5	332:12, 18
322:16	100:17	98:25	283:10	<b>I&amp;P</b> 56:25
355:13	187:12	<b>Hill</b> 8:11	291:22	<b>IA</b> 26:4
<b>hear</b> 257:24	324:7	335:17	298:23	<b>idea</b> 17:19
327:8	358:2	<b>historic...</b>	350:11	47:17 49:9
334:21	<b>helps</b> 43:18	259:8	<b>hosted</b> 117:5	50:14
344:8	43:18	<b>hoax</b> 219:13	<b>hosting</b>	51:11
349:6, 8	44:11	<b>hoses</b> 281:10	160:18	57:25 58:2
<b>heard</b> 22:11	90:24	<b>hold</b> 138:22	<b>hour</b> 319:7	58:12 84:3
134:6	263:20	139:2, 3, 3	<b>hours</b> 175:16	84:10, 13
145:15, 17	317:23	185:7	177:9	84:24
263:8	<b>hereunto</b>	186:18	181:3	89:19 90:8
277:5	374:13	190:22, 24	271:11	108:3
<b>hearing</b> 65:3	<b>hesitant</b>	212:24	349:23	109:1
124:6, 11	317:25	231:18, 21	<b>House</b> 140:4	132:16
290:23	<b>hey</b> 14:12	242:18, 19	140:19	171:15
<b>heavy</b> 367:12	27:2 86:25	242:22	<b>housed</b>	184:23

**BRIAN J. SCULLY 1/12/2023**

185:5,13	59:3 60:13	141:22	301:5	196:12
185:21	87:3 89:24	149:23	308:22	375:16
192:23	233:4	364:7	327:18	<b>indicates</b>
215:23	314:21	<b>implemented</b>	332:7	192:22,23
257:1	361:15	363:19	339:3	253:19
261:13,13	370:10,13	<b>implemen...</b>	<b>included</b>	278:3
346:19	<b>identifying</b>	118:2	39:21	280:9
371:23	191:11	<b>implies</b>	99:16	291:9
<b>identifi...</b>	210:21	222:4	111:21,25	<b>indication</b>
14:1 69:8	232:24	<b>implying</b>	112:4,5	153:2
138:21	370:5	339:10	225:5	<b>indicator</b>
156:15	<b>IG 285:7,8</b>	<b>imposter</b>	235:14	42:19
190:14	<b>Illinois</b>	205:23	247:17	<b>individual</b>
195:1	299:12,22	206:7	276:18	134:24
213:1	<b>image 154:13</b>	<b>in-authen...</b>	301:10,16	193:15
227:10	154:14	239:5	309:13	258:23
243:23	<b>images</b>	<b>in-person</b>	<b>includes</b>	<b>individu...</b>
249:23	330:10	295:15	45:3 48:2	241:22
252:6	<b>imagine</b>	<b>inaccurate</b>	61:4 72:16	<b>individuals</b>
277:17	180:21	321:9	254:16	35:15
301:21	208:18	<b>inauthentic</b>	293:23	38:12
306:19	209:23	41:23 42:3	357:8	179:24
309:21	221:3	42:10,15	<b>including</b>	180:12
319:16	268:9	115:1	67:15	246:19
328:5	274:19	<b>inbox 194:23</b>	206:7	<b>Indraneel</b>
335:13	<b>immediate</b>	212:20	246:24	3:18 11:5
345:21	176:14	227:13	277:8	<b>Indrane...</b>
349:16	314:7	302:2	304:14	3:24
352:14	<b>immediately</b>	319:18	312:13	<b>industry</b>
359:14	110:4	<b>inboxes</b>	321:24	21:4,7
363:7	195:17	189:11	354:22	31:15 78:7
364:12	205:10,17	192:21	359:2	117:14
365:11	293:16	<b>incident</b>	370:22	132:5
368:4	<b>immigration</b>	144:19	371:16	179:2
369:18	220:10	218:19	<b>incorrect</b>	233:13,17
<b>identified</b>	<b>impact 152:8</b>	221:19	119:15	233:19
57:6 85:4	154:4	236:10	<b>increase</b>	237:2
191:14	158:4	264:11	336:24	243:18
192:9	313:1	<b>incidents</b>	<b>increasing</b>	244:13
193:22,24	332:3	109:21	150:15	245:15
233:10	340:13,16	110:1	154:4	253:20,21
276:24	340:21	268:8	<b>incredibly</b>	254:2,15
288:7	343:7	<b>include</b>	304:9	254:21
361:4	<b>imperson...</b>	18:16	<b>independ...</b>	255:21
<b>identify</b>	206:22	50:25	60:7	256:1,8,13
17:4 27:20	207:8	109:12	316:14	257:5,7,8
37:25 38:7	<b>impetus</b>	232:9	317:3	257:17,22
38:9 44:9	356:11	295:19	<b>indicate</b>	257:24
57:10,15	<b>implement</b>	300:1,19	54:19	260:8



**BRIAN J. SCULLY 1/12/2023**

262:9	179:25	154:1,5	320:18	230:1
297:25	193:10	265:25	<b>instances</b>	280:2
343:1	207:9	269:20,25	200:18	283:12
<b>industry...</b>	220:3,7,17	270:5,8,9	<b>institut...</b>	341:19
216:18	220:20,22	270:15	97:8 100:3	360:11
<b>inference</b>	220:22	309:6,7	355:11	362:2,9
245:22	222:19	322:15,17	<b>instruct</b>	368:9
<b>influence</b>	223:5,14	322:20	35:5	<b>intel</b> 259:12
12:5 26:15	224:11	323:6	150:21	332:25
117:25	225:19	327:3,13	152:23	333:9,11
118:7	226:8	327:13,16	153:20	333:22
130:1	254:19	331:18	156:1	334:15
271:6	258:11	332:2,4,6	<b>instruction</b>	<b>intellec...</b>
309:1,8	263:4	332:7	51:2	286:21
330:14	264:10	338:17,18	167:14	<b>intellig...</b>
348:13	278:23	338:19,23	339:17	25:18 26:2
350:15,22	279:11,14	339:1,3,5	<b>instruct...</b>	34:9 36:7
351:14	280:8	339:6,12	156:9	36:8 39:20
356:20	283:15,25	340:9,12	<b>intake</b>	95:15
364:18	287:20,21	340:22	105:17,23	235:4
<b>informal</b>	289:3	341:1,2,4	107:14	244:12
136:4	290:22	341:13	<b>integrity</b>	246:19
<b>information</b>	291:5	<b>infrequent</b>	5:16 48:7	257:2
35:7 39:22	300:25	32:1	48:10,25	258:17,18
40:5,11	301:5	<b>initial</b> 52:4	49:7 51:5	258:20
45:24,25	315:13,16	58:14	51:20 52:1	332:14,22
48:15	315:22	86:10	52:23	<b>intended</b>
59:15 60:4	321:9	89:19	57:25 68:5	283:15
60:6,16,22	323:4,9,15	117:13	69:21 73:3	<b>intending</b>
73:9,17,21	326:12	223:5	73:8 75:7	252:8
74:1,4,6,7	336:2	241:9	78:16 79:6	<b>intensive</b>
74:9 78:21	339:9	<b>initially</b>	79:7 80:3	62:19 63:8
79:5 82:16	357:2,7	101:15	83:20	166:11
87:5 90:15	359:2	<b>initiative</b>	84:25 88:6	173:23
94:7	<b>informat...</b>	9:22 90:11	88:13,18	<b>interact</b>
105:23	17:11	316:5	97:19	278:24
115:7	270:9	<b>Injunction</b>	107:19	279:2
121:21	<b>informed</b>	6:25	126:25	310:20
137:21	72:20	<b>inoffensive</b>	127:7	<b>interacting</b>
140:20	143:21	311:5,6,10	128:11	314:20
147:6,7,16	<b>infrastr...</b>	<b>inputs</b> 109:8	132:11	<b>interaction</b>
148:5	4:6 12:10	<b>inquiry</b>	134:19	75:10
150:20,23	15:24 16:6	208:8	141:3	<b>interact...</b>
151:25	16:9 59:15	<b>Inspector</b>	147:8	24:10
152:22	60:15 61:1	328:12	168:21	51:25 75:7
153:18	110:14	<b>Instagram</b>	181:11,15	117:10
154:6	137:24	146:7	200:16	121:16
165:2,8	141:24	217:11	202:14	<b>interagency</b>
166:8	147:5	285:10	228:8	18:11

**BRIAN J. SCULLY 1/12/2023**

36:25 37:1	196:14	153:16	170:6	263:3
<b>Intercept</b>	200:1	169:12, 15	187:8	<b>involve</b>
9:4 319:20	<b>intern's</b>	169:20	370:5	60:22
<b>interest</b>	182:20	170:1, 16	<b>internships</b>	245:15
9:25 44:10	<b>internal</b>	172:8, 11	51:13	247:21
47:4	108:12	172:11	89:22 90:7	<b>involved</b>
159:14	120:13	182:14	<b>interpret</b>	16:8 21:19
161:6	133:7	185:17	275:6	21:21
341:3, 5	155:20	186:11, 14	371:7, 8	25:12 26:1
374:11	165:17, 21	186:23	<b>interpre...</b>	48:6, 20, 22
<b>interested</b>	329:20, 23	188:5	239:4	51:5 56:4
27:13	<b>internally</b>	195:11	257:21	61:5 73:2
56:19	58:21	196:18	<b>interpreted</b>	75:6 78:2
143:13	<b>internat...</b>	201:25	257:14	80:14, 16
<b>interesting</b>	44:4, 20, 22	361:22	<b>interrog...</b>	80:16
116:3	44:24	362:3	6:25 192:3	81:24 82:3
192:7, 17	338:25	363:12	<b>interrog...</b>	82:6, 7
192:18	<b>internet</b>	<b>interning</b>	189:14	88:10
317:25	50:6 51:8	196:19	190:18	97:24
<b>interest...</b>	51:10, 23	<b>interns</b> 49:9	231:16	100:3
122:11	52:5, 11	49:15	242:15	101:22
355:17	58:9, 11	50:13, 16	243:7	102:5, 9
<b>interfer...</b>	59:7, 9	50:18, 25	353:2	104:15
45:2 83:2	61:7 62:24	51:4, 12, 13	<b>interrupt</b>	113:6
83:3	63:19	51:14, 16	13:6 178:1	114:9
122:14	64:19	51:16, 18	<b>intersti...</b>	117:20
286:22	67:14, 21	51:19 52:4	228:5	134:18, 19
<b>interloc...</b>	70:15, 21	57:3 58:4	<b>interval</b>	134:21, 22
310:5	72:16	58:20 75:9	125:19	153:15
<b>intermit...</b>	76:15 78:5	84:2, 3, 11	<b>intervening</b>	168:3
31:13	78:9 79:14	84:20, 22	89:2	169:18
<b>intern</b>	79:17, 21	84:23 86:7	<b>interview</b>	170:19
166:19	79:25 80:2	86:7, 14, 20	345:23	172:10, 17
167:9, 10	80:17, 21	86:25 87:4	346:1, 3, 5	180:12, 14
167:12	80:24 81:6	94:25 98:6	<b>introduce</b>	184:10
168:22	81:13, 17	170:5, 9, 10	10:18	188:20, 21
169:3, 4, 7	82:2 83:24	170:12, 18	<b>introduc...</b>	189:13
169:21, 23	85:6 89:4	171:15	126:16	192:1
170:24	89:7, 11, 20	184:23	<b>invaded</b>	207:7
171:2, 7, 8	101:14, 21	185:13, 20	325:7	211:18
172:16	101:25	187:5, 22	<b>investig...</b>	215:9
179:19	104:18, 22	197:23	366:19	232:24
182:11, 13	110:18	198:2	<b>investig...</b>	245:13
182:21	112:6, 11	368:15	255:10	256:4
183:14, 20	117:6	371:23	<b>invitation</b>	280:1
185:22, 25	119:9, 20	<b>interns'</b>	153:8	312:8, 11
186:5	129:11	57:25	<b>invite</b> 55:12	318:19
187:11, 13	142:25	58:14	55:17	327:16
188:2, 8	147:18, 21	<b>internship</b>	<b>invites</b>	334:17

**BRIAN J. SCULLY 1/12/2023**

360:10,24	269:19	<b>job</b> 1:21	332:12	262:13
361:25	270:16	11:20,25	<b>joint</b> 207:16	<b>jumping</b> 73:5
362:4,11	272:9	12:8 15:19	233:8	203:25
362:19	290:7	18:10	253:21	204:5
366:13	<b>items</b> 30:18	115:24	254:2	261:24
<b>involvement</b>	30:22,23	116:1	307:22	269:4
49:6,8	34:5	314:7	<b>Joseph</b> 1:9	<b>June</b> 5:17
192:19	268:15	342:23,24	4:20 10:7	55:4 86:10
371:18	272:21	347:16	11:18	86:17
<b>involves</b>		<b>jobs</b> 340:19	375:8	195:14,19
59:21	<b>J</b>	<b>John</b> 3:3	376:3	196:13
81:12	<b>J</b> 1:14 2:1	10:19	<b>Josh</b> 3:6	345:24
<b>involving</b>	5:2,8 6:3	14:12	10:24	352:21
156:20	7:3 8:3	34:18 54:7	<b>JOSHUA</b> 3:17	<b>June/July</b>
278:1	9:3 11:12	82:23	375:5,10	86:12
<b>Iowa</b> 214:13	375:12	125:10	<b>Joshua.e...</b>	<b>junior</b> 10:7
214:17	376:2	138:23	3:23	43:16
<b>Iranian-...</b>	377:5,20	139:2,3	<b>Josiah</b> 42:22	<b>jurisdic...</b>
285:22	<b>Jack</b> 9:24	145:7	166:18,24	17:6
<b>Isabella</b>	188:7	167:19	179:18	114:18
185:25	195:3,5	179:19	184:14	220:16,17
186:3	196:17,20	184:14	191:24	221:11,22
<b>ISAC</b> 59:14	197:18	185:10	192:12	222:1,5,13
59:16,21	198:1	191:25	276:20	<b>jurisdic...</b>
60:14,15	<b>January</b> 1:15	192:12	<b>journalist</b>	57:11,17
60:16	10:3 12:2	194:21	280:10	57:22 87:4
110:15	19:20	198:12,22	<b>JR</b> 1:9 375:8	<b>justice</b> 3:19
<b>issue</b> 208:15	71:16	212:17,17	376:3	11:1,6
289:2,22	88:24	213:7	<b>July</b> 86:17	322:1
324:13	195:19	227:19	98:25	324:11,13
<b>issued</b> 222:1	196:13	231:19	104:25	324:15
310:9	307:11	232:1	269:6	375:5
<b>issues</b> 21:22	330:13	242:19,24	271:24	
34:21 71:4	374:14	249:16	272:6	<b>K</b>
130:24	375:3,12	252:7	274:18	<b>K-theore...</b>
163:8	376:4	253:7	<b>jump</b> 89:14	240:5
234:24	<b>JCDC</b> 307:17	271:10	122:2	<b>Kaitlin</b>
235:24	307:19	276:20	125:1	141:13
237:14	309:9	302:7	126:11	<b>Kansas</b>
239:1	<b>Jefferson</b>	318:21	144:6	375:21
310:21	3:11	334:20	146:20	<b>Kate</b> 72:21
315:14	<b>Jen</b> 191:19	371:11	162:5	87:25
317:14	304:9	<b>John.sau...</b>	173:2,8	360:4
318:6,15	307:2	3:13	271:9	<b>keep</b> 180:18
324:9	311:23	<b>join</b> 38:18	288:15	185:8
342:8	<b>Jessica</b> 4:3	<b>joined</b> 10:21	293:14	271:15
349:12	11:3	35:11	297:7	290:3
<b>item</b> 247:13	<b>Jessica....</b>	36:15	<b>jumped</b> 33:12	<b>Kent</b> 3:5
258:24	4:9	76:14,15	160:13	35:9

**LEXITAS LEGAL**

**BRIAN J. SCULLY 1/12/2023**

<b>kept</b> 165:15	99:19,24	242:1	42:6 43:1	104:20,21
190:6	100:8,10	246:6	46:13 47:7	104:22,24
<b>key</b> 16:13	104:8	255:25	47:10,10	105:5,20
18:11,15	105:2,12	256:2,25	47:16 49:2	105:21,24
189:9	112:9	257:3	53:6 55:22	106:2,9,10
263:3	114:13,20	258:8	55:24 56:6	106:15
276:15,25	114:23	260:21	56:10 57:7	107:6,18
355:11	115:3	263:14	58:23	107:21
<b>kicked</b> 127:1	116:22	266:3	59:11,18	108:5,6,14
<b>Kim</b> 28:6	119:24	267:16	59:18	108:17,23
304:14,18	120:6,7	270:10,14	61:11 62:1	109:25
305:2,4	121:21,22	270:14	65:20,22	110:20,21
353:18	124:14	271:5	65:23	111:5,10
360:22	128:9	289:18	66:20,21	111:20
<b>kind</b> 13:7	132:13	290:18	68:16 69:1	113:10,15
14:14 16:7	133:14	293:4	69:3,4	113:21
18:5 20:7	136:4,17	315:23	70:19	114:4
24:25 25:8	136:24,24	317:22	71:12,24	115:7,22
26:14,16	138:10	318:5,9	72:6 73:20	116:24
27:2,5	141:6,6,7	323:16	73:23	117:8
29:2 30:14	141:9	324:2	74:13	118:13,18
31:18	145:1,5	337:3	75:15	119:14
37:22	147:21,22	344:21	76:19,21	120:24
39:25	148:3,17	347:11	76:24 77:4	121:1,3,6
40:20	149:13	356:6,8	77:15 79:6	121:14,16
41:12,25	150:15	357:20,24	79:9 80:1	121:21,24
42:2,11	152:1,5,13	358:18	80:7,12	121:25
43:21	153:13	<b>kinds</b> 24:9	81:4,5,15	122:24
44:11,17	154:9	49:11	81:15,16	123:2,6,22
45:1 46:3	157:1	215:19	81:25 82:3	123:25
47:4,15,20	161:18	368:22	82:18	124:17,19
47:22 52:8	164:24	<b>Klein</b> 345:24	83:18	124:21,21
52:15,19	174:12	<b>knew</b> 100:17	84:16 85:3	127:11,11
52:25	175:16	117:2,6,9	85:16,24	127:16
55:16 56:3	178:5,7	176:24	85:25 86:5	128:3,19
57:4 58:1	182:4	192:18	86:11 88:3	128:21
58:22	187:2,13	295:22	88:5,10,17	129:6,10
60:10 62:8	187:25	313:19	89:1,12,25	129:14,22
63:14	207:4	<b>know</b> 13:2	90:2,3,4	132:13
64:22,25	211:11,18	16:23 22:8	91:21	133:9
65:25 66:2	217:3	22:21 25:5	94:11,16	134:12,22
66:4 67:12	225:13	27:4,9	95:5 98:13	137:5,8
68:17 71:2	234:15,25	28:18 29:1	98:15 99:4	140:19
71:3 77:16	235:3	29:6 30:19	99:6,17,23	142:11,14
80:1 81:4	237:6	31:1,23	100:17	142:20,22
81:10,22	239:3,13	32:12,12	101:5	142:22
82:1,13	240:1,2,15	32:25 34:5	102:17	143:9,11
84:13 88:9	240:17	39:3,4,24	103:17	144:1,1,2
94:12 98:3	241:12	41:10 42:4	104:8,10	145:12,12

**LEXITAS LEGAL**

**BRIAN J. SCULLY 1/12/2023**

145:19,21	203:8	273:12,16	327:1,5,19	76:23 77:8
146:9,14	204:14	274:13,17	327:23	77:8,9,17
146:18	205:2,3	274:20,21	328:20	77:17,20
148:16,20	207:22	274:22,23	330:1	78:4,9
148:22	208:22	275:1,16	332:3	191:20
149:19	209:20	275:25	333:12,15	284:14
152:17	210:7,18	278:14,16	334:10,13	285:2,13
154:16	210:25	279:20,22	336:19,25	285:18
158:1,3,22	211:2,2,11	280:1,4,6	337:5,9,18	286:5
159:3	211:13	280:22	337:21	288:20
162:11	212:9	282:7,11	338:4,6,10	290:1,6
163:6,25	213:14	283:2,19	339:10	291:11
164:9,9	215:20	283:23	340:22	340:5
165:25	216:7,11	285:2,8	342:8,9	<b>Krebs'</b> 290:4
168:5,18	216:14	286:10	343:12	<b>Krebs's</b>
168:25,25	220:3	287:12	350:19,25	77:24
169:13,18	221:6	291:7	351:12,14	289:23
169:21	224:13,14	293:19,21	351:17	<b>Krebs-St...</b>
172:13	225:12,14	293:21	352:5,9,10	197:12
173:24	225:18	294:1,13	352:12	<b>Krebs/St...</b>
174:19	228:23	294:18	353:17	76:23
176:8,16	231:9,12	295:1,22	354:1,1,18	<b>Kris</b> 308:6
176:18	234:24	296:24	356:2,5,10	308:10,11
177:8,13	235:6	298:14	356:14,23	<b>Kristi</b> 228:7
177:15,16	236:20	301:1	356:23	
177:22	237:10,20	307:21	358:13,16	<b>L</b>
178:13,17	238:1,2,3	308:10	359:1,21	<b>L</b> 3:20 375:6
179:3,8	238:5,18	309:1,3,12	359:24	<b>L-i-m-b-i-k</b>
180:3	238:18,20	309:15,17	360:7,15	155:4
181:19	239:2,17	310:10,11	360:16,18	<b>L-o-w-a-r-y</b>
182:3,4,23	240:5,10	310:14,15	360:21	183:18
182:23,24	240:19	310:17,18	362:10,12	<b>Lab</b> 47:9
183:24	241:13	310:24	362:12	48:22
185:22	244:24	311:6,12	363:18,21	<b>label</b> 200:15
187:7,12	248:3	311:16	363:22,23	224:17
187:19,25	252:16	312:18	363:25	283:14
188:6,6,9	256:20	313:6,13	364:3,6	<b>labeled</b>
188:14	258:3	313:18,19	365:5,7,24	226:19
190:2,3,23	259:3,4,16	314:6,8	367:8,15	231:5
192:16	260:7	315:12	367:20,24	292:9,14
193:6,14	261:21	316:1,22	368:1	292:16
193:25	262:10,13	317:1,6	369:10	<b>labeling</b>
194:8,17	263:19,20	318:8,13	<b>knowledge</b>	288:6
194:18	264:7,9	318:16,19	56:7 61:9	<b>lack</b> 80:4
197:18	269:2	321:15,16	146:19	122:21
198:7,8,11	270:24	321:23	172:12	145:11
198:14	271:8	324:19	324:14	149:17
201:3,6	272:14,24	326:19,20	<b>known</b> 274:10	178:15
202:12,17	273:4,5,9	326:23	<b>Krebs</b> 76:7,8	195:25

**LEXITAS LEGAL**

**BRIAN J. SCULLY 1/12/2023**

197:1	297:24	274:9	84:14	5:15
214:22,23	298:23	275:7,13	141:7	<b>like-minded</b>
244:20	299:16,21	275:16,20	<b>let's</b> 34:22	97:8
245:7	300:11	<b>Leaked</b> 9:5	69:9 83:7	<b>liking</b>
304:21	350:4	319:21	146:20	346:25
313:7	351:12	<b>leaker</b>	151:3	<b>Limbik</b> 155:2
333:19	<b>law</b> 95:13	274:11	172:23	155:10
350:23	245:24	<b>learn</b> 46:3	173:2,3,8	<b>limit</b> 127:7
353:24	250:4,16	47:20	183:4	231:6,9
354:13	250:21,22	<b>learned</b>	197:25	<b>limited</b>
355:5	251:2	54:13 71:3	198:9	36:10
356:22	320:21	84:14	217:2	232:10
359:22	366:5,8,14	141:7	231:15	<b>line</b> 85:14
361:13	<b>lawyer</b> 92:9	144:10	243:25	103:8
368:20,21	<b>lead</b> 16:2	247:19	271:9,19	148:22
<b>lacks</b> 204:24	18:7,10	<b>learning</b>	276:1	202:5,7
329:11	19:9 21:7	143:18	277:19	250:8,12
<b>landed</b> 164:7	28:17 29:2	<b>leave</b> 18:23	285:15	250:16,22
<b>large</b> 305:20	36:1 42:12	19:17	288:15	255:22
305:24	42:23	28:12 65:6	289:6	273:15
<b>larger</b> 14:19	43:24 54:5	88:21	291:15	285:7
181:15	78:7	299:3	294:4	299:15
<b>lasted</b>	117:16	331:1	301:23	376:5,9,13
325:12	118:8	336:12	309:23	376:17,21
<b>late</b> 22:7,16	325:11	<b>led</b> 326:21	330:4	<b>lines</b> 43:17
22:25 70:9	332:25	<b>left</b> 43:24	362:20	58:8 86:25
104:25	342:15	76:13	<b>letter</b> 167:5	133:12
292:5	370:9,18	88:23	<b>letting</b>	207:11
293:5	<b>lead-up</b> 38:8	167:23	294:1	216:24
367:5	298:2	197:19	<b>level</b> 37:22	235:2
<b>lateral</b>	<b>leader</b>	319:7	45:1 56:5	286:15,18
144:17,17	118:10	<b>legal</b> 4:20	153:22	327:6
<b>Laura</b> 29:16	<b>leadership</b>	10:15,16	154:10	333:25
30:6,10,10	97:5	92:5,9,12	182:16	340:15
236:17	317:23	92:18,20	258:23	365:5
248:13	326:12	93:11	259:17	<b>link</b> 285:9
270:20	371:1	94:15	318:12	320:23
<b>Lauren</b> 18:6	<b>leading</b> 33:4	95:21 96:3	333:8,13	<b>LinkedIn</b>
28:12	<b>leads</b> 43:20	368:22	<b>levels</b>	9:24 38:17
75:18	44:4 311:9	370:22	146:23	195:6
191:21	<b>leak</b> 236:7	371:16	<b>Lexitas</b>	196:3,5,9
255:19	236:14,19	375:1,24	10:16	196:11
260:4	237:4,14	<b>lengthy</b>	375:1,24	233:25
269:13	246:1,13	139:13	<b>liaisons</b>	<b>links</b> 96:23
294:8	247:7,21	343:24	264:16	146:1
295:2,7,17	250:18,24	<b>lesson</b>	267:18	<b>list</b> 72:11
296:6,15	251:13,22	144:10	<b>lie</b> 348:7	87:25
296:22	254:17,23	<b>lessons</b>	349:2	165:19
297:1,10	255:2,11	54:13	<b>Lightning</b>	232:11

**LEXITAS LEGAL**

**BRIAN J. SCULLY 1/12/2023**

233:8, 21	265:25	87:10	168:3	279:4
243:2	282:2	141:2	170:20	304:3
264:3	292:22	177:2	175:23	316:15
276:17	299:17	187:25	179:13	322:24
285:22	316:2	276:4	180:13	324:8
338:9	317:6	314:8	212:21	340:17
339:3	337:19	319:4	213:13	342:21
342:14	341:8	349:20	224:10	348:21
354:2	<b>live</b> 198:23	372:4	232:18, 23	349:6
361:3, 4, 9	344:14	<b>longer</b> 18:20	291:4	<b>lots</b> 342:6
361:16, 20	<b>loading</b>	167:22	316:13	349:12
<b>listed</b> 43:23	345:17	<b>look</b> 14:7	<b>looks</b> 82:24	<b>Louisiana</b>
110:11, 24	<b>local</b> 24:5	58:9 69:9	161:12, 17	1:2 10:11
111:2, 5, 6	54:20, 23	88:1 90:13	162:8	<b>love</b> 307:16
112:22	57:18	90:22	173:18	<b>low</b> 57:8, 9
180:12	58:23 60:1	122:9	175:25	<b>Lowary</b>
191:19	60:23 61:3	156:17, 25	176:5	183:16
192:14	79:3 85:1	157:1, 16	195:10, 18	184:10, 22
233:6	91:19	162:19	197:11	185:15
274:14	93:16 96:6	173:12	198:19	192:1
280:5	96:16	175:22	199:22	193:1, 22
<b>listen</b> 13:10	101:10	186:2	214:17	196:25
<b>listen-only</b>	106:11	190:22	218:22	197:7
28:6, 7, 11	148:5	206:14	223:2	276:21
<b>lists</b> 15:16	149:16	215:1	269:16	<b>lower</b> 292:22
105:12	150:20	217:3	280:19	361:3
192:11	164:9, 14	219:20	282:10, 13	<b>Luke</b> 28:16
280:8	204:17	222:8	283:24	28:22 29:1
<b>literally</b>	207:7	253:24	294:7	
160:13	215:10	273:23	295:3	<b>M</b>
<b>Litigation</b>	222:1	274:20	297:18	<b>ma'am</b> 372:23
4:5	265:20	276:15	<b>loom</b> 8:10	373:2
<b>little</b> 14:11	266:7	278:2	<b>loop</b> 107:9	<b>machines</b>
14:15	296:17	281:4	<b>looping</b>	292:23
22:19	298:9	296:5	203:9	<b>mad</b> 281:10
26:22 73:7	299:12, 21	309:23	308:6	<b>Magnets</b> 5:12
83:1 101:6	300:20	312:22	<b>loose</b> 293:20	<b>main</b> 21:17
102:12	369:3	335:2	<b>loss</b> 341:24	236:5, 5
130:20	<b>location</b>	338:24	342:4, 9	279:18
143:4	263:23	339:2	<b>lot</b> 40:6	306:17
146:18	281:9	340:1	45:4 125:7	<b>mainstream</b>
172:25	<b>Locust</b>	359:20	159:23	357:9, 16
181:7	375:21	<b>looked</b>	162:12	359:3
182:18	<b>logged</b> 190:7	314:20	177:21	<b>maintain</b>
197:10	<b>logistics</b>	340:2	235:16	146:22
220:5	30:17	<b>looking</b> 15:7	239:14	170:6
235:17	<b>long</b> 5:9	41:2 59:2	257:2	<b>maintained</b>
240:14	11:19, 24	141:14	260:15	120:9
263:11	27:17 46:3	162:14	261:19	<b>major</b> 105:13

**LEXITAS LEGAL**

**BRIAN J. SCULLY 1/12/2023**

110:7	26:10	98:9 113:9	313:11,13	300:19
111:6,12	90:18 91:6	117:4	314:12	301:6,9
126:24	94:22 95:6	120:2,18	317:20	303:20,20
<b>majority</b>	278:22	129:17	<b>Matt's</b> 85:20	305:9,13
18:12	<b>mandates</b>	130:23	<b>matter</b> 10:6	312:23
131:3	47:16	142:24	92:23	313:5
180:21	<b>manner</b> 318:9	191:20	361:5,16	316:9
254:6	<b>March</b> 71:16	217:23	<b>matters</b> 4:5	318:10
<b>making</b> 49:19	336:12	218:3,5,19	344:18	320:10
56:1 85:7	<b>marked</b> 13:25	219:5	350:15,22	323:7
92:21	69:7	237:19	351:14	325:9,10
122:18	138:20	251:7,12	356:20	325:11
128:5	156:14	253:16	<b>Matthew</b> 4:11	326:2,5
144:9	190:13	271:25	283:10	330:16,21
173:16	194:25	283:9	<b>matthew....</b>	331:5,16
176:24	212:25	284:5	4:15	331:19,23
178:8,21	227:9	305:5	<b>mature</b> 46:2	337:4,15
211:21	243:22	313:11,13	<b>May/June</b>	338:22
238:18	249:22	314:12	53:19	342:23
269:10	252:6,21	317:21	<b>MD</b> 20:17,21	343:19,19
286:7,25	277:16	318:13	354:8,15	343:22
301:2	301:20	<b>Masterson's</b>	354:20,22	344:22
340:18	306:18	129:19	355:10,19	346:16
<b>mal-info...</b>	309:20	<b>material</b>	357:2,7	347:23
5:20 8:15	319:15	246:22	<b>MDM</b> 11:21	348:12
15:17,23	328:4	<b>maternity</b>	16:5,14	353:3,7,10
20:1,14	335:12	18:23	19:10	353:12,13
143:15,19	345:20	19:17	20:12	355:24
145:20	349:15	331:1	39:15 42:9	356:12
340:11	352:13	<b>Matt</b> 11:4	44:9,16	357:20,21
341:18	359:13	75:10,17	45:6 56:20	357:25
343:6,10	363:6	80:13	72:24	358:6,11
<b>manage</b> 16:1	364:11	81:17	75:20	358:24
16:2 43:4	365:10	82:18	118:8	359:1
64:25	368:3	83:16	143:21	366:3,23
<b>managed</b>	369:17	88:14,23	153:25	367:12
18:13	<b>Marybeth</b>	98:14	154:4	371:20
364:7	71:10	120:2,12	166:9,12	<b>MDM-related</b>
<b>management</b>	<b>Masterson</b>	130:3,7,22	171:18,20	329:15
11:22	75:11	142:24	188:11	<b>MDM-spec...</b>
308:25	80:13,23	191:20	189:7	113:12
309:7	81:17	217:23,25	233:8,8	<b>mean</b> 17:2
327:15	82:19	218:3,5,19	274:2	34:2 48:11
343:17	83:16 84:4	219:5	278:25	49:3 55:13
<b>manages</b>	85:17	237:19	285:24	62:8 66:13
42:25	86:13	271:25,25	295:5,11	69:3 71:25
<b>managing</b>	87:22	283:9	295:20	74:5,15
262:21	88:14,18	284:5	297:3,5	82:12
<b>mandate</b>	88:21 89:9	305:5	298:4	103:20



**BRIAN J. SCULLY 1/12/2023**

105:4, 25	<b>meaning</b>	94:13	241:6	358:12
108:4	287:3	105:14	242:16	359:3, 4
114:2	298:9	107:20	244:18	363:16
115:11, 21	313:1	108:2	245:4, 16	364:21
121:19	<b>means</b> 118:13	109:13, 13	246:23	365:2
131:17	273:17	114:24	247:25	366:2, 5, 25
133:17, 18	275:14, 25	118:25	254:18	<b>medium</b> 359:9
135:24	285:8	120:22	256:14	<b>meet</b> 133:2
143:12	289:14	122:18	257:17	239:25
148:15	298:14	123:5, 17	258:2, 5, 12	241:10
149:8	309:2	126:19	258:14	<b>meeting</b> 21:6
151:21	350:14	127:5, 20	259:4	24:13
152:16	351:14, 17	129:12	261:4	30:17
160:17	<b>meant</b> 133:4	131:20	263:24	31:14
165:6	142:10, 11	132:2, 12	265:17, 22	36:21, 22
169:4	218:9	132:17	266:9	37:2, 4
174:8	223:22	134:4	268:23	38:23
175:2, 9	232:16	138:11	269:1	47:20
176:8, 16	241:1	144:4, 24	274:5, 8	75:16
182:2	257:15	146:3	277:9	78:10
183:3	334:24	151:8	278:7, 13	85:21 86:2
189:5	351:13	152:18	286:20, 24	86:13, 17
193:24	354:19	153:15	286:24	86:23
197:17	358:16	157:10	290:13, 25	87:10 99:1
204:14	<b>measures</b>	163:19	291:25	99:4, 7, 12
207:3	355:13	164:11, 13	293:5, 6	99:17
211:7	<b>mechanism</b>	165:4	296:16	100:22
227:4, 23	61:16	168:7	300:18	103:8
227:24	<b>meddling</b>	172:5, 18	305:18	117:15, 17
231:8	175:1	180:16	314:19, 21	140:1
236:4	<b>media</b> 17:4, 8	189:25	317:13	233:7, 12
248:6	17:10, 13	192:2	318:4	233:13, 17
257:5	17:16	193:3, 9	326:14, 24	243:15, 18
270:8	18:16, 21	200:21	327:3, 9, 18	248:25
273:7, 22	20:8 21:1	208:23	333:16	253:25
274:7	21:5, 23	210:12	339:10, 23	254:7
275:1	23:21 24:2	214:3	340:4, 6, 8	256:3
280:22	24:5, 10, 13	220:4, 6, 25	341:14, 16	259:20
281:17	27:1, 23	221:20	347:1	262:9
287:8	38:13 39:2	222:17	350:15, 21	269:14, 17
293:18	39:8 57:21	223:20	350:21	269:18
298:13	58:17 59:3	228:9	351:3, 7, 13	270:1, 3, 21
309:3	64:2 66:5	229:4, 8	351:24	270:25
316:17	66:17 67:1	232:8, 25	352:11	272:5
326:16	67:18 68:8	233:18, 22	356:19, 19	274:18
338:9	73:12, 12	233:24, 25	357:8, 9, 10	275:3
341:12	73:18	235:13	357:15, 16	309:13, 16
358:7, 13	78:21 79:6	237:3	357:20, 21	337:25
366:21	93:21 94:7	239:11, 21	357:23	<b>meetings</b>

**BRIAN J. SCULLY 1/12/2023**

21:4,9,10	241:4,5,15	<b>memory's</b>	257:1	322:19
24:19,23	241:18	22:19	268:21	336:13
25:7,12,15	242:16	101:6	282:14	<b>mid-October</b>
25:16 26:8	243:8,18	<b>mention</b>	283:25	174:21
28:1,15,23	243:21	20:11	303:21,23	<b>middle</b> 110:8
29:11,15	244:11,17	38:11	314:23	157:17
29:23	245:3,14	39:23,25	316:3,4	162:20
30:15 31:6	245:14,19	103:11	320:12	208:7
31:10	245:24	110:5	322:14	278:3
32:10,13	246:8,14	131:25	336:22	<b>midnight</b>
32:16 33:4	246:18	159:4	349:10	175:13
33:8,20,24	247:2,11	247:24	353:18	226:18
34:6,10	247:20,25	263:9	355:21	292:1
35:16 36:3	248:15,24	<b>mentioned</b>	356:3	293:16
36:12,18	249:11	24:12	362:16	<b>midterms</b>
36:19,20	251:13,23	29:10 39:1	367:10	8:10 298:2
37:7,15	254:4,24	40:23 46:9	<b>merely</b>	<b>mimic</b> 134:11
38:7,14	255:3	48:1,18	220:21	<b>mind</b> 99:8
39:9 45:21	256:2	56:18 59:5	<b>merging</b>	180:19
45:23	258:2,10	59:6 60:11	110:2	346:15
50:11	260:5	63:7,16	<b>messages</b>	357:8
52:10	269:6	72:15	8:22	359:2
74:23	272:19,21	74:23	106:12	<b>mine</b> 71:9
77:21 78:1	306:2,9	80:13	120:15	83:22
78:10,16	310:23	85:13,23	178:4	180:22
102:9,12	317:16	99:19	309:25	<b>minority</b>
102:14,15	323:2	100:5	<b>met</b> 141:6	122:19
102:22	353:23	101:17	238:4	<b>minute</b> 99:9
103:12	361:6,11	102:8	239:25	99:15
112:1	<b>member</b>	111:20	338:4,10	107:13
117:14,19	183:22	112:16,23	<b>META</b> 297:25	156:17
127:19,22	325:10	117:4	<b>method</b>	292:24
128:14,20	<b>members</b> 49:2	131:4,19	290:15	345:17
128:22	97:25	139:5,6	<b>methodology</b>	<b>minutes</b>
132:4,6,21	166:12	140:5,23	154:18,20	87:13
132:23	180:7	153:24	<b>meting</b>	175:25
133:7,8,12	263:9	157:4	295:15	206:2
178:25	264:24	159:1	<b>Michigan</b>	224:16
216:18	279:16	170:3	46:25 47:1	226:15,18
232:8,25	326:7	183:11	<b>Microchips</b>	271:16
233:4,6	359:20,25	184:5	5:12	274:14
234:21	<b>Memes</b> 5:11	187:14	<b>Microsoft</b>	276:3
236:3,8,23	<b>memories</b>	189:21	38:16,18	282:5
237:15	247:13	190:5	38:19	292:4
238:5,6,7	<b>memory</b>	193:14	88:22,25	318:25
238:10,13	230:22,23	198:3	233:24	319:6,7
238:15	247:14	240:13	297:11,25	349:23
239:9,20	255:1	251:3	<b>mid</b> 22:20	<b>mis</b> 5:20
240:6,9	258:24	252:2	23:9,10	8:14 15:17

**LEXITAS LEGAL**

**BRIAN J. SCULLY 1/12/2023**

19:25	127:8	293:5	<b>mix</b> 333:5	<b>MOLA_DEF...</b>
20:14, 18	130:17, 24	310:21	<b>mixed</b> 64:9	8:6
40:13	132:14, 19	311:3	<b>Mm-hmm</b> 23:18	<b>MOLA_DEF...</b>
42:11, 12	137:21	317:14	110:13	7:11
42:14, 16	138:6, 11	318:6	139:15	<b>MOLA_DEF...</b>
57:20	141:22	322:6	163:1, 12	7:13
58:24	142:3, 15	323:11	166:25	<b>MOLA_DEF...</b>
90:19	144:3	324:12	274:16	7:9
91:17 92:3	149:15, 23	335:20, 25	300:16	<b>MOLA_DEF...</b>
92:15 93:1	150:17	336:5, 16	308:24	9:14
93:20	151:7	338:1, 8	330:17	<b>MOLA_DEF...</b>
94:12, 23	157:3, 6, 9	357:14	350:7	9:19
95:7 96:10	158:6, 14	363:13, 20	365:15	<b>MOLA_DEF...</b>
96:18	160:7	364:8, 21	370:7	8:23
126:22	161:9, 21	365:2, 16	<b>Mm-mmm</b> 111:1	<b>moment</b>
127:12	164:10	<b>misleading</b>	<b>MO</b> 375:21	352:18
143:14, 18	165:3	283:15	<b>mode</b> 28:6, 7	<b>Monday</b> 373:4
145:20	169:19	336:2	28:11	<b>money</b> 61:16
147:3	173:13, 24	<b>misreading</b>	263:21	62:3, 3
151:23	178:23	160:14	<b>model</b> 154:12	110:20, 22
314:14	179:4, 15	<b>missed</b> 233:9	<b>modeling</b>	342:18
315:3	198:20	<b>missing</b>	155:9	<b>monitor</b>
340:11	200:3	282:19	<b>moderated</b>	57:20 59:3
341:17	201:2, 23	<b>mission</b>	17:24	90:18 91:6
343:6, 9	208:10	26:19 29:7	<b>moderation</b>	91:17 92:2
347:21	210:25	62:25 63:2	17:18	92:15 93:1
348:20	213:17	153:25	40:15	94:23 95:6
354:9, 15	215:9	309:5	123:7	151:14
363:15	216:12	316:12	128:10, 16	174:10
370:14	217:9	338:23	260:10, 13	175:17
371:2	225:1, 17	343:2	260:23	325:20
<b>mischara...</b>	226:8	<b>Missouri</b> 1:5	284:7	<b>monitored</b>
23:6 97:21	228:17	3:7, 11	289:15	108:2
345:7	229:10	10:6, 20, 23	296:3	<b>monitoring</b>
<b>misinfor...</b>	232:9	35:10	<b>modulation</b>	57:15
5:10 8:4	233:1	375:8	23:22, 22	144:24
8:13 21:22	235:12, 13	376:3	289:9	150:16
39:7 41:18	235:25	<b>mistake</b>	<b>MOLA_DEF...</b>	176:6, 9
41:20 42:1	238:8	232:4	7:18	178:22
42:8 43:10	239:1, 10	<b>mistaken</b>	<b>MOLA_DEF...</b>	201:2
45:17 77:3	239:22	232:16	6:5	225:15
91:6	243:10	<b>misunder...</b>	<b>MOLA_DEF...</b>	287:19
106:23	260:24	229:5	6:21	326:8
114:24	261:5	<b>mitigate</b>	<b>MOLA_DEF...</b>	348:5
118:3	264:23	16:15	6:14	<b>Monkey</b> 324:6
120:8, 10	265:5, 16	343:20	<b>MOLA_DEF...</b>	<b>Monroe</b> 1:3
124:24	268:4	358:3, 23	9:21	10:11
125:23	278:12	<b>Mitigation</b>	<b>MOLA_DEF...</b>	<b>month</b> 31:24
126:4	287:21	106:19	8:21	248:24

**LEXITAS LEGAL**

**BRIAN J. SCULLY 1/12/2023**

<b>monthly</b> 24:17 31:21 32:3 233:14 234:3, 5, 9 234:16 255:21 256:3 310:23	<b>multitude</b> 340:20, 24	259:5 286:7, 11 286:17, 19 287:4, 9, 13 288:3, 21 291:11 323:23 340:8	33:3, 14 34:9 35:6 50:8, 9 71:8, 9, 15 71:17, 18 101:16, 17 101:19 103:13 135:25 136:8, 14 178:11 244:12 248:19 332:8 336:7 342:1, 5	264:19 300:25 319:9 348:7 349:2 372:15
<b>months</b> 19:8 24:11 196:6, 10 196:13 248:24 325:12	<b>mystery</b> 337:19	<b>narratives</b> 109:22 110:2 144:3 151:14 152:1, 8 155:7 256:8, 14 256:21 257:18 258:4, 13 259:2 323:17 324:8	<b>needed</b> 127:12 174:10 215:14 216:9 220:6	<b>needed</b> 127:12 174:10 215:14 216:9 220:6
<b>morning</b> 173:18 175:5 176:1 282:4 286:5	<b>N</b>	<b>narratives</b> 109:22 110:2 144:3 151:14 152:1, 8 155:7 256:8, 14 256:21 257:18 258:4, 13 259:2 323:17 324:8	<b>NATO</b> 44:25 45:12 <b>nature</b> 69:4 113:18 139:9 145:13 169:17 203:23 262:23 322:2 325:3 327:5 371:25	<b>needle</b> 81:5 81:10 <b>needs</b> 9:8 57:4 295:10 328:12, 24 329:23
<b>mouth</b> 69:6 <b>move</b> 179:5 291:15 301:23 <b>moved</b> 64:3 336:25 <b>moving</b> 172:25 208:3 282:1 308:15	<b>name</b> 10:14 10:15 11:17 32:20 35:20 36:1 54:6, 7 76:22 103:2, 3 166:20 167:5, 6, 10 167:11 171:7, 10 172:16, 19 172:21 186:1 187:18 194:4 279:25 376:2, 3 377:11	<b>NASED</b> 103:13 103:23 104:2, 23 107:25 112:1 263:23 264:6, 22 267:6 268:25	<b>NAV</b> 263:7 <b>near</b> 292:1 293:16	<b>needle</b> 81:5 81:10 <b>needs</b> 9:8 57:4 295:10 328:12, 24 329:23
<b>MS-ISAC</b> 60:19 <b>multi-state</b> 59:14 <b>multilat...</b> 45:1, 12 <b>multiple</b> 59:22 201:10 230:20 245:14 247:10 359:10 363:16 <b>multistate</b> 60:14 61:2 61:6	<b>named</b> 179:20 182:12 285:21 <b>names</b> 29:3 30:9 50:17 50:20 100:5 167:18 188:24 189:2, 4, 6 189:9 192:6 276:18, 23 <b>narrative</b> 5:12 56:16 154:4 219:10, 16	<b>NASOS</b> 103:23 <b>NASS</b> 103:25 104:3, 23 107:25 112:1 263:24 264:6, 22 267:6 268:25 <b>Nathaniel</b> 310:18 312:6 <b>nation's</b> 337:25 338:7 <b>national</b> 11:22 16:5 20:5 33:1	<b>nature</b> 69:4 113:18 139:9 145:13 169:17 203:23 262:23 322:2 325:3 327:5 371:25 <b>NAV</b> 263:7 <b>near</b> 292:1 293:16 <b>necessarily</b> 36:18 58:5 62:18 65:13 76:11 100:7 149:11 151:24 348:25 <b>necessary</b> 258:22 368:23 377:9 <b>need</b> 34:19 100:17 199:21 227:22	<b>never</b> 27:18 133:4 240:7 242:3 <b>new</b> 41:5 44:9 114:19 142:14 188:19 286:15 290:7, 8 299:12, 22 301:24 305:4 312:22 313:5 336:21 <b>news</b> 109:13 124:16 302:3 334:12

**BRIAN J. SCULLY 1/12/2023**

357:10	<b>noticed</b>	272:9	153:6	6:23 156:8
358:6	228:16	331:9	161:25	215:3
359:3	<b>notifica...</b>	340:12	178:14,15	<b>Observatory</b>
<b>night</b> 175:1	178:5	<b>numbers</b>	179:21	51:8,10,23
175:8,10	<b>notified</b>	162:11	194:14	52:6 58:9
175:12	165:13	211:1,5,11	195:25	58:12
179:7	<b>notifies</b>	<b>numeral</b>	196:4	70:15,21
291:20,21	177:3	141:16	197:1	72:16
292:6	<b>notify</b> 67:16	<b>numerical</b>	198:5	76:15 78:5
293:6	68:7 129:4	14:5	201:4	78:9 80:18
<b>nights</b>	140:18		202:15	80:21,24
173:25	160:8	<b>O</b>	204:12,20	81:7,13,18
<b>No's</b> 252:5	<b>notifying</b>	<b>O</b> 4:1 5:1	204:23	82:2 83:24
<b>nod</b> 12:24	179:24	6:1 7:1	212:2	85:6 89:4
<b>non-profit</b>	<b>notion</b> 94:20	8:1 9:1	214:22	89:7,11,21
47:7 59:13	216:15	10:1	226:25	102:1
148:3	<b>novels</b> 43:3	<b>Oberes</b>	228:18	104:18,23
<b>nongover...</b>	330:10	157:18,25	230:19	117:6
267:11	<b>November</b>	<b>object</b>	231:10	142:25
<b>nongover...</b>	213:15,17	152:20	244:20	169:12,16
45:9,13	214:13	155:25	245:7	169:20
<b>normal</b> 26:10	217:8	<b>objection</b>	258:6	170:1,16
130:6	223:4	23:2,5	273:1	172:8,12
201:7	226:6	53:1 71:20	283:21	182:14
306:9,10	284:24	72:3 77:10	294:16,23	185:17
<b>normally</b>	286:4	77:19 80:4	294:24	186:11,14
41:25	291:18	87:16 92:4	298:11	186:24
165:18	332:12	92:17 93:2	304:20,21	188:5
178:3	334:11	93:22	310:12,13	195:11
270:2	335:15	94:14	313:7	196:18
333:8	336:5	95:20,24	316:19	361:23
<b>Northwest</b>	337:5	96:25	324:24	362:4
3:20 375:6	<b>NRMC</b> 9:22	97:20	333:18	<b>observer</b>
<b>notarized</b>	<b>NSA</b> 286:13	98:11	339:13,19	332:24
375:19	286:16	108:20	341:6	<b>obtain</b> 323:9
<b>notary</b> 2:8	<b>NSD</b> 33:7	111:8	344:25	<b>obtained</b>
374:21	<b>number</b> 10:8	115:9,15	345:6	246:22
375:18	113:22	115:20	350:23	<b>obviously</b>
377:23	160:22	116:17	351:15	12:19 16:1
<b>notation</b>	162:5,22	118:16	352:7	16:19,23
165:14	171:3,7,8	122:21	353:24	17:23
<b>note</b> 178:3	172:16	126:5	354:12	28:11
201:14	190:2	130:19	355:5	38:15 42:6
287:22	201:16	142:6	356:21	51:12
<b>noted</b> 337:24	210:20	145:3,6,10	358:14	77:24 87:7
<b>notes</b> 109:18	214:20,20	146:16	359:5,22	87:21 88:9
<b>notice</b>	214:21	148:8	360:19	107:24
202:24	217:16	149:17	361:13	120:12
203:4	256:10	150:18	<b>objections</b>	175:11

**BRIAN J. SCULLY 1/12/2023**

182:17	245:6,16	332:11	261:1,3,14	15:18 19:7
184:7	248:17	334:2	261:19,23	23:13
194:10	251:18,21	360:17	265:21	34:12
210:15	332:11,19	366:12	266:1,7	44:19
244:25	<b>office</b> 3:7	<b>officially</b>	295:11,20	61:11
245:12	4:12 10:20	89:12	297:2,5,12	87:23
264:4	10:23 11:6	336:11	297:23	88:12
275:16	12:10 26:2	<b>officials</b>	298:2,9,10	89:24 91:2
282:17	34:8 35:11	8:9 16:25	298:14,17	97:4
298:13	44:24	24:1,1,5	299:2,12	100:19
324:19	204:7	45:15	299:22	103:20
351:1	205:12	52:12	300:20,24	104:1,6
359:10	206:6,15	54:18,21	301:8	109:10
367:25	206:19	54:24 57:4	305:8	114:7
<b>occur</b> 24:16	214:13,18	57:8,19	306:15	115:18
53:18 55:3	215:25	58:24 60:1	320:17	119:5
70:6,8	216:1	60:23 61:2	321:1	125:15,16
86:3 87:10	225:2	61:5 62:20	340:18	125:17
246:2	244:11	63:12,24	363:14	126:13
268:18	311:15,19	64:1 73:10	364:20	130:15
334:3	312:10	73:16 75:3	365:1	131:1,25
<b>occurred</b>	328:11	78:20 79:4	366:17	135:6
78:4	333:9,11	79:10,12	372:2	141:20,20
104:11	334:1	80:2 83:23	<b>oh</b> 19:21	144:14
138:14	375:20	87:1 96:7	29:24 89:1	145:23
200:19	<b>officer</b>	96:17	89:5	146:12,21
246:8	280:12	100:18,21	131:19,25	146:22
264:11	289:9	101:11	161:14	150:14
309:16	374:3	102:10	162:17	151:11
327:23	<b>officers</b>	106:1,4,11	163:15	158:2,17
<b>occurring</b>	216:5,5	106:13	167:19	160:21
235:18	<b>offices</b> 57:8	110:5	183:4	162:10
246:7	57:13	119:23	192:8	167:8,16
279:7	90:16	120:4,5,15	225:25	167:24
<b>October</b> 5:21	215:23	123:2	227:21	170:13,23
24:18	<b>official</b>	131:7,24	232:3,16	171:2
156:19	17:4 49:1	148:6	241:3	173:7,11
157:2	50:7 67:10	149:16	249:7	173:12
168:4	68:14	164:5,21	253:4	183:3
173:14	163:22,24	204:18	271:2	184:25
198:19	164:9,14	207:8	282:22	186:5
199:6	165:9,11	215:10,12	297:16	189:13
208:21	180:1	215:24	302:7	190:17
246:4	220:7,23	216:4,8,21	318:24	191:1,6
<b>odd</b> 29:8	221:4,18	216:22	363:5	194:24,24
<b>ODNI</b> 25:23	221:21,24	223:5	<b>OIG</b> 9:8	198:15
34:8 35:15	251:17	242:11	328:16	205:15
36:2 37:14	281:17	260:11,16	<b>okay</b> 13:9	206:4
117:20	331:19	260:20	14:24 15:7	207:20

**BRIAN J. SCULLY 1/12/2023**

208:6, 20	299:20, 23	300:19	148:23	159:18
209:14	302:11	301:16	318:8	304:5
210:19	306:23	<b>one-pagers</b>	<b>operated</b>	<b>ops</b> 119:24
211:9	308:5	295:23	53:6	267:10, 15
212:23	309:24	296:2, 20	155:16	267:21, 24
214:7, 11	320:1	298:1	368:24	<b>option</b> 85:23
215:7	328:10	<b>ones</b> 38:20	<b>operating</b>	<b>options</b>
216:11	329:5	114:2, 3	56:11	216:10
217:2	330:8	121:17	95:16	<b>oral</b> 135:7
219:25	332:9	168:3	148:20	<b>order</b> 14:5
223:17	335:4, 8	185:3	<b>operation</b>	<b>ordinary</b>
224:5	344:11	189:17, 20	247:21	178:12
225:14	345:18	228:16	262:17, 24	<b>Oregon</b>
226:3, 5	348:11	233:9	264:22	201:23
227:16	349:24	234:16	265:9, 10	<b>org</b> 15:8, 12
231:25	354:6	268:17	267:5	18:2 22:12
232:17, 21	355:9	279:19	<b>operational</b>	42:21
232:22	356:25	306:17	98:20, 24	130:8, 13
243:4	359:17	348:22	155:18	166:17
244:4	368:7	<b>ongoing</b>	340:13	167:4
245:23	369:12	364:24	342:13, 16	171:21
246:17	373:3	366:18	<b>operations</b>	<b>organiza...</b>
247:18	<b>omitted</b>	<b>online</b> 94:8	39:22	49:24 62:2
248:8	215:5	114:23	96:11, 19	147:23
250:2, 14	<b>On-call</b>	150:16	179:8	148:19
251:10	107:14	151:15, 23	236:7, 7, 14	369:9
253:7	<b>once</b> 81:22	155:8	236:19	<b>organiza...</b>
255:17	203:16	158:14	237:4	9:23 130:4
256:7, 12	204:1	195:6	246:1, 13	<b>organiza...</b>
259:25	213:20	228:17	247:7	16:21
262:16	299:10	305:24	250:18, 24	45:10, 12
265:8	333:7	336:2	251:13, 22	47:14, 16
269:11, 18	<b>one's</b> 35:20	354:3	254:17, 23	48:5, 13, 17
271:22	35:20, 21	357:11	255:2, 12	50:2 73:11
275:21	<b>one-on-one</b>	359:4	264:15	148:19
280:7, 16	241:11	364:19	278:23	262:21
281:14	<b>one-page</b>	365:1	279:15	323:5, 6
283:2	253:10	<b>oops</b> 346:8	309:1, 8	<b>original</b>
284:22	260:9, 13	<b>open</b> 16:22	312:5	375:13
285:25	260:21, 22	164:2	340:14	<b>originated</b>
286:2, 2	<b>one-pager</b>	281:9	342:20	90:8 94:25
287:2, 17	260:6	325:21	<b>opportun...</b>	123:8
290:24	294:21	326:8, 9	317:8	171:15
294:6	296:8, 11	<b>opening</b>	<b>opportunity</b>	184:23
295:2, 17	296:15	345:18	13:19	185:13, 21
296:14	297:1, 12	<b>operate</b>	234:18	198:2
297:19, 22	297:22	52:25 53:4	<b>opposed</b>	228:14
297:23	298:16	61:23 62:7	91:18	371:23
298:21	299:2, 7, 21	110:19	92:24	<b>originates</b>

**BRIAN J. SCULLY 1/12/2023**

95:12		173:3, 4, 5	285:25	322:7
329:3		173:9, 10	288:16, 17	<b>panels</b>
<b>originating</b>	<b>P</b> 3:1, 1 4:1	173:11, 20	289:19	187:14
83:19	4:1 10:1	191:3, 6, 8	290:6, 8, 13	<b>paragraph</b>
<b>originator</b>	11:21	195:9	290:19, 21	110:4
201:13	<b>P-a-t-t-o-n</b>	197:11	291:1, 8, 12	147:2
<b>origins</b>	32:21	198:9, 11	291:15, 16	150:2
321:24	<b>p.m</b> 157:2	198:16	293:8	192:6, 8
322:7	173:19	199:16	294:4	244:8, 9
<b>outcome</b>	175:25	201:17, 22	295:2	245:23
374:12	177:3	203:14, 15	296:6	304:7
<b>outcomes</b>	183:9	204:1, 1, 5	297:8, 9	305:15, 16
27:22	209:9, 12	204:7	298:19	330:10
354:25	276:7	205:8, 10	299:14, 15	332:10
<b>Outline</b> 9:5	291:20	206:9	305:15	335:23
319:21	292:5, 23	208:3, 4	307:6	336:15
<b>outlining</b>	292:24	213:14	310:6	337:23
321:6	362:23	214:7, 9	313:10	348:3
<b>outputs</b>	363:1	216:25	315:17	361:15
109:8	372:12	222:20	320:2, 15	<b>parentheses</b>
<b>outreach</b>	373:9	224:21, 22	321:3, 3	281:10
18:13, 15	<b>P.O</b> 3:10	225:5, 11	330:2, 4, 5	<b>parody</b>
272:1	<b>PA</b> 217:10	225:16, 20	332:10	205:24
<b>outside</b>	<b>page</b> 5:2, 8	225:25	346:7	206:6
134:3	6:3 7:3	226:2, 4	348:2	281:10
151:6	8:3 9:3	227:17	354:4	<b>part</b> 11:22
353:22	15:16	228:2	356:25	20:2 51:23
<b>overall</b> 96:8	72:11 73:7	231:22, 25	364:16	61:8 63:25
<b>overlapped</b>	87:23	232:3, 13	365:17	75:16, 20
195:22	89:14, 16	242:20, 25	366:1	78:23
<b>overseas</b>	90:21	247:19	368:11, 12	104:7
41:11	98:19	249:5, 25	370:1, 2	106:7
278:20, 23	105:8, 11	251:15, 15	375:14, 18	110:22
279:5, 8, 9	108:12, 24	251:16	375:20	115:25
280:19	109:2, 11	260:3	376:5, 9, 13	128:7, 21
<b>oversee</b>	110:9	261:25	376:17, 21	147:22
25:15	117:22	262:4	<b>pages</b> 1:22	149:10
<b>overseeing</b>	122:2, 5, 10	269:4, 5, 9	160:22	169:4, 5, 7
59:21	125:2, 5, 14	271:9, 20	206:5	169:24
<b>oversees</b>	126:11, 12	271:21, 24	208:4	181:14
59:13	141:15	278:2	269:11	189:7
<b>overtaxing</b>	144:6, 7	280:7, 14	276:15	192:3
211:15	145:23	280:15	285:15	193:3, 5
<b>overview</b>	146:20	281:2, 4, 6	291:16	201:7
136:17	149:22	281:15	332:9	203:12
<b>overwhelmed</b>	156:25	282:3	<b>paid</b> 203:2	264:21
342:17, 18	157:17	283:7, 7	<b>pandemic</b>	281:20
<b>overwhel...</b>	160:22, 25	284:9, 19	264:20	290:5
65:1	162:7, 9, 11	284:21	321:25	311:1
	162:16, 20			



**BRIAN J. SCULLY 1/12/2023**

322:24	181:19,21	369:10,13	364:18	291:17
323:21	334:13	<b>partners</b>	<b>pass</b> 106:5	294:5
325:9	<b>particip...</b>	16:20	123:16	297:8
338:23	126:18	18:11,12	163:8	298:20
342:23	354:23	21:5 37:1	265:5	299:16
347:15	<b>particular</b>	44:5,20,22	<b>passed</b> 56:23	330:5,6,8
362:1	11:25	46:11	162:24	370:2
<b>part-</b> 330:19	23:20	109:17	<b>passing</b>	<b>peers</b> 244:13
<b>part-time</b>	30:18,22	110:1	141:10	<b>penalty</b>
170:6,12	31:9 42:17	204:9	<b>patient</b>	377:12
184:3	65:8 74:10	224:2	280:12	<b>pending</b>
<b>participant</b>	85:22	228:8	<b>Patton</b> 32:17	255:9
354:2	112:15	235:2	32:17	<b>Pennsylv...</b>
<b>particip...</b>	136:5	264:6,12	<b>pay</b> 196:21	218:18
72:11,12	152:7	267:11	197:20	219:19,22
128:23	154:14	298:1	<b>PDF</b> 89:16,17	223:4,13
<b>participate</b>	159:24	369:2,6	122:6	223:21,25
55:12,16	179:11	<b>partnership</b>	125:5,12	<b>people</b> 18:4
131:11	209:1	5:16 48:7	125:14	29:19 30:5
132:7	211:16	48:10,25	126:12	36:2 46:24
323:1	258:14,16	49:2,7	144:8	54:8 56:4
333:5,6,13	287:9	51:6,20,24	160:25	103:4
353:5,10	341:20	52:2,24	162:7,9,11	112:10,13
<b>particip...</b>	346:8,9,11	58:1,6	173:6,10	112:14
25:22 26:3	359:9,12	68:5 69:21	198:11,16	114:1,5
28:2,23	<b>particul...</b>	73:3,8	201:18	115:6,12
29:14 33:7	33:23	75:8 78:16	203:14	134:18,19
34:10	52:16	79:8 80:3	204:8	140:18
35:15	56:19 82:6	83:20	205:10	152:18
38:14,17	174:17	84:25 85:8	206:10,11	154:23
38:23 39:3	239:24	88:6,13,19	208:5	159:23
55:14 71:5	256:19	89:19	214:10	168:2
77:21	266:11	97:19	217:1	174:8,22
78:10	279:5	99:21,24	222:21	175:16
132:3	286:5	100:9,11	224:22	176:5
238:12	289:22	107:19	225:25	178:12
274:17	299:3	132:11	226:4	179:3
309:18	344:17	134:20	227:17	181:22
326:4	366:10	141:4	228:3	189:7
333:2	369:2	147:8	251:16	191:11,24
353:21	<b>parties</b>	168:21	261:25	192:9,11
<b>particip...</b>	10:18	181:12,15	269:5,9	192:19
28:2	374:10	202:14	271:21	193:1,18
310:22	<b>partisan</b>	228:8	280:15	193:19,21
353:9,14	357:10	230:2	281:4,6	201:1
353:16,23	358:12	280:2	283:8	255:20
<b>particip...</b>	359:3	360:11	284:19,21	259:3
33:4 39:5	<b>partner</b> 96:7	362:2,9	286:1	263:25
76:4	97:8	<b>parts</b> 30:5	288:16	285:22

**BRIAN J. SCULLY 1/12/2023**

291:2	152:2	344:16,23	10:21	17:16
297:11	<b>person</b> 20:7	<b>picked</b> 372:2	35:11	18:17,21
316:8	53:25	<b>piece</b> 220:13	<b>plan</b> 8:8 9:6	20:8 21:1
324:7	117:18	<b>Pierce</b>	32:9	21:6,23
331:4	129:24	183:15	269:23	23:21 24:2
336:21	171:3	184:10,20	<b>planned</b>	24:6,11,14
337:4,15	219:11	184:22	136:17	25:1,9
342:17,19	264:3	191:25	307:12	27:1 38:13
344:14	<b>person's</b>	193:1,22	<b>planning</b>	39:8 40:2
347:20	36:1 103:1	196:25	295:19	40:4,7,8
348:4,21	<b>personally</b>	197:7	<b>plans</b> 54:12	40:10,15
349:4,8	236:15	276:21	54:15	40:24
358:2,18	238:3	<b>pilighting</b>	319:22	41:19,21
358:21	245:13	151:21,22	321:8	42:6 58:18
360:2	<b>perspective</b>	<b>pilot</b> 151:18	367:21	59:4 64:5
364:23	24:25	152:15,19	<b>platform</b>	64:14,22
<b>perceive</b>	39:15	153:14	21:11 64:3	65:1,12
96:23	42:10	154:7	65:16	66:5 67:1
<b>percent</b>	45:25 46:7	155:6,11	66:17	67:7 73:12
26:18,24	47:13	155:17	67:10,18	73:18
61:15	234:22	<b>piloted</b>	68:9	78:22 79:7
122:12,13	257:25	151:16	120:25	94:8
137:18	315:12,15	<b>piloting</b>	126:17	105:14
149:12	323:2	151:13,22	133:2,9	106:8
169:16	325:25	152:2,5	134:4	107:2,10
<b>percentage</b>	326:1	<b>pilots</b>	146:4	119:1,11
123:3	367:12	155:14	160:9	120:22
<b>perform</b>	<b>pertained</b>	<b>pinging</b>	161:11,22	121:7,8
265:4	30:15	176:20	163:2	122:18
<b>performed</b>	<b>phone</b> 99:9	<b>Pinterest</b>	164:2,7,12	123:6,17
63:16	99:12,15	233:24	165:4,7,16	126:24
<b>performing</b>	227:5	<b>place</b> 56:25	168:7,16	127:5
161:19	293:12	135:25	179:14	128:2,25
<b>performs</b>	<b>phones</b>	232:8	180:8,9	129:12
63:20	174:10	291:5	200:21	131:21
<b>period</b> 20:24	175:17	314:12	208:24	132:2,12
21:20	176:6	325:17	220:25	132:17
28:23	<b>phonetic</b>	334:4	222:17	133:5,16
31:11 41:7	47:14	351:24	223:21	138:12
162:3	71:10	356:12	241:11,22	158:5
180:22	141:13	363:15	278:7	160:1,3,5
246:2	<b>phrase</b> 56:22	<b>placed</b>	287:14	160:8,10
<b>periodic...</b>	<b>physical</b>	128:13,15	300:18	160:14,17
30:4 162:4	235:18,23	<b>places</b>	306:14	161:10,23
164:15	263:23	220:11	352:11	163:19
165:20	270:12	<b>plaintiff</b>	357:20	164:19
<b>perjury</b>	342:12	3:2 10:7	<b>platform's</b>	168:11
377:12	<b>pick</b> 32:4	<b>plaintiffs</b>	261:6	172:5,18
<b>perking</b>	174:6	1:7 6:23	<b>platforms</b>	178:21,21

**BRIAN J. SCULLY 1/12/2023**

179:7, 10	315:2	<b>plus</b> 193:1	284:7	62:16
179:14, 24	316:14	331:1, 11	289:15	153:8
180:16	317:4, 7, 13	<b>POCs</b> 350:14	296:3	242:2
184:9, 11	317:23	<b>point</b> 34:1	<b>policy</b> 12:9	367:25
189:25	318:4, 11	58:4 64:21	126:13	368:1
192:2	326:14, 24	101:9, 23	129:4, 12	<b>positions</b>
193:3, 10	327:9, 18	102:4	133:2	337:8
203:13	340:6	103:3	134:1, 4	<b>possibility</b>
210:13	348:5, 6, 8	174:7	200:16	99:20
212:9	348:24	233:12	209:21	<b>possible</b>
214:3	349:2	234:21	261:6	22:18 39:6
220:6, 18	350:21	255:25	283:12, 13	75:14 95:9
221:20	351:25	262:8	311:16	98:10
229:9	356:19	275:18	312:4, 9, 11	129:6
232:9, 25	357:9	290:18, 19	312:12	133:18
233:18, 22	363:17	290:21	332:8	147:19
235:6, 9, 13	364:21	291:19	338:25	190:12
237:3	365:2	323:20	<b>political</b>	193:20
239:21	366:5, 25	326:11	130:4, 7, 12	198:1
240:1, 7	<b>play</b> 59:1	327:2	246:20	200:22
241:8	62:18, 22	337:3	313:14, 17	208:11
242:16	64:11	354:7	364:15	210:18
244:19	100:13	355:9	<b>Politics</b> 8:7	216:10, 20
245:4, 16	152:13	358:1	<b>poll</b> 217:10	224:14
246:24	168:9	<b>points</b> 128:5	219:1, 11	236:11, 16
248:1	316:13	135:19	235:20	237:8, 17
254:18	317:8, 10	234:14	339:11	237:21
256:4	317:18	243:3	<b>popped</b>	246:10
257:18	<b>played</b>	272:22	234:15	248:10
258:2, 12	149:20	350:14	<b>popping</b> 27:3	254:16
260:17, 19	182:5	351:2	302:2	255:10, 11
261:11, 21	345:10	<b>police</b> 9:6	<b>portal</b> 8:5	256:18
262:18	<b>playing</b> 19:4	305:17	320:20	257:24
263:24	63:6	319:22	363:13, 20	290:5
265:2, 6, 17	311:24	<b>policies</b>	364:8, 20	294:20
265:22, 24	<b>please</b> 10:17	17:18, 21	365:1	295:5
266:9	11:9, 16	21:13	<b>portfolio</b>	358:10
268:19, 24	130:21	23:22	20:3	<b>possibly</b>
269:1	145:7	121:23	<b>portion</b>	22:25
277:9	167:10	123:7	129:1	23:13
290:13, 15	185:9	126:17, 25	257:23	231:14
290:25	205:22	127:7, 11	270:5	<b>post</b> 198:23
291:3, 4, 7	218:23	127:14, 25	<b>portions</b>	225:4
292:1	308:7	128:10, 17	70:1	227:20
293:6, 15	339:18, 22	132:13, 18	<b>portrayed</b>	228:9
296:16	361:16	133:5, 10	229:6	229:4, 9, 13
305:19, 24	375:11, 15	133:17	<b>poses</b> 56:16	339:25
306:4, 6	375:19	177:5	<b>position</b>	344:15
314:13, 21	<b>plura</b> 250:5	260:23	35:21, 21	345:11

**LEXITAS LEGAL**

**BRIAN J. SCULLY 1/12/2023**

<b>post-ele...</b> 227:6	161:19 162:3	99:18	<b>prior</b> 21:8 24:21	113:23 124:5,15
<b>posted</b> 82:19 116:9 280:20 290:14	200:25 209:21 210:14	<b>presiden...</b> 147:4 246:3	36:12,17 36:19 74:21 117:8	124:17 174:20 180:25 181:4
<b>posting</b> 159:25 274:6,8 291:3 340:7	<b>pre-marked</b> 14:6	<b>presumably</b> 204:11 298:9	241:20 314:3 332:11	211:8 230:25 235:7
<b>postings</b> 259:4 341:14,16	<b>pre-mate...</b> 28:12	<b>presume</b> 308:19	<b>priorities</b> 321:7	241:17,18 243:19
<b>posts</b> 82:14 82:14,18 114:17 115:7 116:13 225:15 339:9,23 340:1,3	<b>prebunk</b> 315:3,9	<b>pretty</b> 56:14 56:21 180:5	<b>priority</b> 16:3	271:12 316:4
<b>potential</b> 17:13 25:3 27:15 38:2 155:7 312:22 313:4,5 342:15,21 361:4	<b>prebunk/...</b> 314:15	<b>Prebunking</b> 315:20	<b>privacy</b> 152:4,12 155:18 165:18	323:25 327:24 331:8,12 331:14
<b>potentially</b> 19:18 39:21 40:21 57:16 87:6 100:2 140:5 277:11 315:18 343:20 357:21 361:5	<b>preceden...</b> 336:1	<b>predated</b> 364:22	<b>private</b> 16:20 18:11 44:7 47:12 221:15 225:4,10 225:16 308:3 314:7 327:14	337:10 341:23 346:2 369:10 372:2
<b>Pox</b> 324:6	<b>predict</b> 152:8 154:3	<b>prevent</b> 344:22	<b>privilege</b> 34:16,21 150:21,24 152:23 153:1,19 156:1	<b>problem</b> 65:25 304:9,14 359:1
<b>practical</b> 92:23 93:11	<b>predictive</b> 152:10 154:12 155:9	<b>previous</b> 23:6 97:21 117:2 251:24 313:16,22 314:3,7,10 345:7	<b>Pro-Trump</b> 217:12 218:25	<b>problems</b> 234:25 357:7
<b>practice</b> 62:6 65:19 66:13,18	<b>Prelimin...</b> 6:24	<b>previously</b> 190:5 205:24 236:21	<b>procedure</b> 297:2	<b>proceed</b> 11:11 35:8
	<b>prep</b> 255:21 269:16,18	<b>primaries</b> 28:5	<b>proceedings</b> 374:4,6,7	<b>process</b> 43:4 43:5,5 49:19 64:7 64:8 65:12 65:14 67:12 83:25 85:4 85:7 106:7 118:2,15 150:20
	<b>preparation</b> 233:7 243:15,17	<b>primarily</b> 46:7 54:1 174:3		
	<b>preparatory</b> 37:6 256:1	<b>primary</b> 75:10 83:21 308:22		
	<b>prepared</b> 194:3 254:22 361:17 370:10,13	<b>principal</b> 29:2 103:5 120:4 167:19 180:23		
	<b>preparing</b> 188:21 190:9 254:16	<b>principally</b> 16:11 38:25 49:16,16 63:9		
	<b>present</b> 4:19 10:17 20:24 28:25 99:1 99:13,13			

**LEXITAS LEGAL**

**BRIAN J. SCULLY 1/12/2023**

152:22	16:12,13	366:11	24:25 25:8	53:9 56:12
153:1,19	16:17	<b>promoting</b>	25:17	56:13
156:1	39:16,18	77:5	40:21	72:20
164:23	43:1,4,7,9	<b>prompt</b>	61:23 62:1	74:24 81:2
201:7	44:12	293:23	94:7 98:20	81:20
211:17	56:21	294:1	135:13,19	82:10,11
239:25	131:5	<b>promptly</b>	220:3,18	82:22
240:11,18	207:16	176:7,21	222:13	112:25
240:19	298:8	<b>prompts</b>	234:23	113:1,7,18
241:1,2	303:15,23	256:8	257:3	114:8
274:25	303:24	257:5	258:11	115:14,17
282:7	316:2,3	<b>proposal</b>	260:9	127:20
283:4,17	333:23	363:11,18	261:10	131:5,6
297:5	343:5	363:23	290:22	134:14
300:19	<b>Professi...</b>	364:7,19	296:7,16	137:11,14
320:16	2:6 374:3	364:22	298:3	138:3,19
337:19	<b>professor</b>	<b>proposed</b>	315:13,16	138:25
356:8	360:8	272:4	323:14	145:1,1
<b>processes</b>	<b>profile</b> 9:24	275:4	325:24	220:16
177:21	195:6	336:24	326:1	221:1,3,10
203:6	196:3,5,9	<b>proposes</b>	361:10,17	221:14
240:23,24	196:11	272:5	<b>provided</b>	222:14
<b>produce</b>	<b>program</b>	<b>protect</b> 8:8	61:12,13	238:22,25
295:18	148:4	339:2	64:4 88:18	254:22
<b>produced</b>	152:17	<b>protected</b>	109:8	283:16,25
156:20	279:12	35:7	188:24	305:10
191:16	<b>programming</b>	<b>protecting</b>	189:2,6,9	306:3,10
192:10	155:15	338:22	209:17	322:16
277:11	<b>project</b> 5:11	<b>Protection</b>	220:12	323:5,5
310:1	51:10	12:11	223:5,20	335:16
<b>product</b>	134:7,9,15	<b>Protentis</b>	299:20	341:19,24
28:18	135:8,22	18:7 19:15	323:12	347:25
43:12	136:10,18	31:5 36:13	325:20	348:1
131:6	137:4,17	42:22	<b>provides</b>	355:13
137:24	139:8	75:18	61:10	368:8
143:24	141:3,14	191:21	317:7	369:21
154:24	144:2	255:20	320:23	374:21
155:10	153:14	260:4	<b>providing</b>	375:18
172:2	368:10	269:13	128:23	377:23
187:11,15	<b>Project's</b>	294:8	<b>public</b> 2:8	<b>publicly</b>
243:13	138:19,25	295:2	9:25 16:12	43:8 47:19
295:10	<b>projects</b>	297:10	21:12,12	82:15
322:19,25	187:13	298:23	21:13 40:6	145:13
355:23	188:16	350:4	40:18,19	190:19
356:11	<b>prolifer...</b>	351:12	40:21,24	195:5
<b>production</b>	336:1	352:3	41:14	284:2
42:25	<b>promote</b>	<b>Protentis's</b>	46:15,15	354:3
276:14	330:15	21:1	50:24	<b>published</b>
<b>products</b>	<b>promoted</b>	<b>provide</b>	52:17 53:8	26:12

**BRIAN J. SCULLY 1/12/2023**

<b>pull</b> 14:9,16 138:16 154:14 212:15 222:6 252:20 253:5	46:14 47:18 53:8 59:6 62:11 62:12 69:5 74:24 82:10,13 101:13,15 101:23,24 101:25 102:4,24 103:16,19 103:21 104:2,4 112:12,13 112:24 120:14 129:7 165:14 207:15,15 221:10 222:6 231:15 260:21 272:18,25 273:13 290:7 301:11,17 303:14,22 303:24 319:19 322:18 325:23 345:19 351:6,24 363:9 368:10 369:20	156:18 242:12 284:1 306:10 328:7 335:10	339:18 345:9 348:4 349:11 354:10 361:18 364:4 371:11	<b>quietly</b> 320:3 <b>quote</b> 338:15 338:20 344:5,13 344:20 348:10,18 349:11 364:20 <b>quotes</b> 322:3 370:3 <b>quoting</b> 368:13
<b>pulled</b> 221:2 <b>pulling</b> 242:19 302:1 352:16 359:16	112:12,13 112:24 120:14 129:7 165:14 207:15,15 221:10 222:6 231:15 260:21 272:18,25 273:13 290:7 301:11,17 303:14,22 303:24 319:19 322:18 325:23 345:19 351:6,24 363:9 368:10 369:20	<hr/> <b>Q</b> <hr/> <b>quadrennial</b> 321:5,13 321:15 <b>qualifies</b> 351:11 <b>quarterly</b> 32:1,13 234:4,9 <b>question</b> 13:10,11 34:13,14 34:19 35:5 51:2 66:21 94:5 114:18 116:18 119:15 134:13 146:4,12 151:1 153:11,22 167:14 179:23 180:10,24 181:6 185:9 186:19,20 197:6 213:8 218:24 220:10 223:18,19 243:5 250:12,15 258:8 275:21 278:22 291:14 299:25 330:6 331:12	<b>questioning</b> 276:12 <b>questions</b> 13:2,19,21 13:22 41:2 46:14 57:3 74:25 81:2 81:20 112:25 114:10,20 116:7,8 122:1 127:23 181:7 234:19 251:25 257:7,16 257:22,25 260:16 261:20 271:15 298:25 339:22 356:9 370:23 371:17 372:6,8 373:4 <b>queue</b> 105:18 105:23 <b>quick</b> 34:13 36:9 125:3 282:5,6 <b>quickly</b> 34:20 47:10 176:10 177:18,20 179:5 228:10 229:5	<b>quietly</b> 320:3 <b>quote</b> 338:15 338:20 344:5,13 344:20 348:10,18 349:11 364:20 <b>quotes</b> 322:3 370:3 <b>quoting</b> 368:13
<b>pulls</b> 44:8 <b>pundit</b> 123:20,23 124:23 125:18,22 126:3	112:12,13 112:24 120:14 129:7 165:14 207:15,15 221:10 222:6 231:15 260:21 272:18,25 273:13 290:7 301:11,17 303:14,22 303:24 319:19 322:18 325:23 345:19 351:6,24 363:9 368:10 369:20	<b>R</b> <hr/> <b>R</b> R1:9 3:1 4:1 10:1,7 375:8 376:3	81:20 112:25 114:10,20 116:7,8 122:1 127:23 181:7 234:19 251:25 257:7,16 257:22,25 260:16 261:20 271:15 298:25 339:22 356:9 370:23 371:17 372:6,8 373:4 <b>queue</b> 105:18 105:23 <b>quick</b> 34:13 36:9 125:3 282:5,6 <b>quickly</b> 34:20 47:10 176:10 177:18,20 179:5 228:10 229:5	<b>race</b> 258:23 <b>races</b> 256:9 256:15 258:5,14 258:14,16 <b>racial</b> 322:1 324:11,13 324:15 <b>radar</b> 124:3 124:10 <b>radio</b> 357:10 359:4 <b>raise</b> 30:19 30:22,24 37:17 99:20 128:25 236:18 <b>raised</b> 31:2 247:10 255:2 355:17 <b>raising</b> 124:23 126:2 236:13,16 251:22 261:21 352:5 <b>Ramaswami</b>
<b>purchase</b> 372:22,24	221:10 222:6 231:15 260:21 272:18,25 273:13 290:7 301:11,17 303:14,22 303:24 319:19 322:18 325:23 345:19 351:6,24 363:9 368:10 369:20			
<b>purpose</b> 16:4 17:9 24:20 24:22 27:6 45:16,20 45:22,23 103:7 260:12 296:25	231:15 260:21 272:18,25 273:13 290:7 301:11,17 303:14,22 303:24 319:19 322:18 325:23 345:19 351:6,24 363:9 368:10 369:20			
<b>purposes</b> 17:12 155:18	319:19 322:18 325:23 345:19 351:6,24 363:9 368:10 369:20			
<b>pursuant</b> 2:2 200:16	319:19 322:18 325:23 345:19 351:6,24 363:9 368:10 369:20			
<b>push</b> 64:2 164:4 165:7,10 175:11,14 175:18 183:15 293:13	319:19 322:18 325:23 345:19 351:6,24 363:9 368:10 369:20			
<b>pushed</b> 300:18 318:5	319:19 322:18 325:23 345:19 351:6,24 363:9 368:10 369:20			
<b>pushing</b> 147:8	319:19 322:18 325:23 345:19 351:6,24 363:9 368:10 369:20			
<b>put</b> 26:9 40:6,24 41:15	319:19 322:18 325:23 345:19 351:6,24 363:9 368:10 369:20			
	<b>puts</b> 47:3 <b>putting</b> 21:12 30:20 34:5 43:1 52:9 52:16 56:24 84:24 85:11 97:18 100:14 112:5,10			

**BRIAN J. SCULLY 1/12/2023**

187:20	371:9,9	292:4	113:5,13	251:25
<b>ramped</b> 174:1	372:9	374:20	113:16,19	259:15
<b>ramping</b>	373:12	<b>reason</b> 56:11	113:20	265:19
105:2,5	375:15	68:12	114:3	268:13
<b>random</b> 333:4	376:6,10	266:22	116:19	270:20,23
333:5	376:14,18	273:13	117:14	272:14
<b>range</b> 46:20	376:22	314:25	119:12	284:8,17
171:25	377:6	376:7,11	120:15	285:6,21
231:13	<b>reading</b> 91:1	376:15,19	121:1	285:23
321:9	95:25	376:23	124:9,15	287:1
342:21	124:19	<b>reasonable</b>	126:2,8,10	289:11
<b>rapid</b> 147:9	150:6	230:25	127:14	290:1,4
<b>rationale</b>	159:20	<b>reasons</b>	128:1,13	301:18
68:18	160:12	130:5	128:18	303:17
<b>re-ask</b>	161:16	<b>recall</b> 21:24	129:5,8	321:20
185:10	211:20	22:9,17	132:20	334:15
371:11	275:17	24:8 26:20	133:6,13	345:25
<b>re-tweeting</b>	347:3,6	27:9,18,24	133:20,23	346:4
346:23	<b>reads</b> 207:5	29:3,16	134:2,23	351:9
<b>reach</b> 116:7	228:11	31:7,8	135:18	356:16
221:25	361:15	32:19	137:5,15	362:17
222:12	<b>ready</b> 40:18	33:22 34:3	139:20	371:24
340:5	<b>reaffirm</b>	37:18,20	140:16,23	<b>recalling</b>
351:5	242:2	38:5,12,20	141:8	52:20
<b>reached</b> 65:8	<b>real</b> 78:12	39:5 41:9	142:17,19	268:8
116:16	371:16	54:2,9	143:6,7	<b>receive</b>
228:23	<b>reality</b>	55:19	151:5	71:11
307:10	290:6,7,9	56:13	168:15	79:25
350:20	291:8	65:18,24	179:6	106:4
351:1	315:17	66:6 67:14	182:2,15	119:7,8
356:15	<b>realize</b>	67:20	189:15	123:4
<b>reaching</b>	199:1	75:14 76:3	190:11,12	131:13
224:2	<b>really</b> 30:7	76:3 78:2	194:6	174:3,23
316:14	30:8 77:11	78:3 80:25	200:23	178:5
317:3	104:10	82:20	203:11,21	252:19
351:23	188:1,16	86:15,17	209:25	260:15
<b>read</b> 11:2	196:21	87:20	210:14	262:25
69:24 70:1	197:20,22	90:12 95:2	211:12,14	264:23
90:23 91:8	203:25	95:9 97:13	214:4	266:6
96:20	253:3	97:15,17	216:19,23	<b>received</b>
143:2,4,5	297:17	97:23	218:13	22:13
143:6,7,9	317:23,25	99:16	235:9	23:25
143:11,12	327:5	100:4,5	236:5,9,15	49:13 52:7
219:21	344:16,16	101:3,20	237:21	67:9 68:14
275:18	372:1	102:23	238:11,22	71:7 79:20
287:15	<b>realtime</b> 2:7	103:1,18	239:6	109:8
299:18	2:7 73:9	103:18	246:6,9	120:5
355:7	73:17,21	106:6,24	247:1,10	123:1
361:12	78:21 79:4	112:12,21	247:24	137:10

**LEXITAS LEGAL**

**BRIAN J. SCULLY 1/12/2023**

157:13	184:21	<b>records</b>	214:25	262:16
159:6	237:6,17	188:25	240:19,23	<b>reiterate</b>
165:8	333:20	<b>recurring</b>	250:10,11	240:9
168:9	367:7	233:5,12	269:23	<b>rejects</b> 8:8
175:13	<b>recollec...</b>	<b>recycled</b>	272:13	<b>relate</b> 19:24
176:24	41:7 55:6	324:9	275:17	41:17
177:1,24	255:5	<b>red</b> 106:17	285:10	156:21
178:3	<b>recommend</b>	<b>redacted</b>	286:25	159:17
180:4,9	295:4	214:20	295:25	240:5
193:12	<b>recommen...</b>	<b>Reddit</b> 38:16	316:25	<b>related</b> 6:25
200:3,10	141:21	233:23	<b>refers</b> 20:17	26:12 77:2
231:2	150:12	<b>reduce</b> 309:5	23:19	81:18
252:23	329:20	316:10	146:14	122:12,13
294:1	330:3	332:2	250:4	122:19
306:12	355:18	346:11,17	255:21	127:15
366:17	358:25	347:16,23	291:12	130:17,24
<b>receives</b>	<b>recommen...</b>	<b>reduced</b>	<b>reflect</b>	133:14,15
149:14	141:19	374:8	259:5	137:3,25
<b>receiving</b>	149:23	<b>refer</b> 20:18	<b>reflected</b>	138:5,15
63:23 64:1	330:3	182:6	201:9	143:14
107:24	354:6	233:16	<b>reflects</b>	150:23
166:10	<b>recommen...</b>	270:9	47:4	159:19
182:8	328:23	354:15	<b>refresh</b>	161:10
215:9,18	355:3	366:8	230:22	235:12,25
307:4	357:1	<b>reference</b>	255:1	238:7,25
<b>recess</b> 34:20	<b>recommends</b>	73:15	<b>refreshes</b>	263:6
35:1 83:11	142:2	105:25	230:23	273:20
183:7	150:3	144:13,15	<b>refusing</b>	285:24
209:10	<b>record</b> 10:3	145:24,25	167:13	312:12
276:8	11:17	149:22	<b>regarding</b>	323:1
319:12	34:23,25	370:25	244:14	324:15
362:24	35:3,9	<b>referenced</b>	278:19	325:8
<b>recipients</b>	83:2,6,8	201:13	<b>regardless</b>	342:8
214:20	83:10,13	<b>referencing</b>	296:25	362:8
299:13,23	183:4,6,9	91:22	358:9	366:19
<b>recognize</b>	183:11	118:19,20	<b>Registered</b>	371:15
15:8	209:5,7,9	<b>referred</b>	2:6 374:2	374:10
<b>Recognizing</b>	209:12	60:18 98:5	<b>regular</b> 21:3	<b>relates</b>
126:21	276:5,7,10	201:10	40:7,24	157:9
<b>recollec...</b>	276:13	<b>referring</b>	82:13,14	162:19
38:11	319:4,9,11	20:14 43:7	127:19	279:5
67:12	319:14	57:1 73:23	128:3	317:15
101:9	349:21	78:24	141:17	<b>relating</b>
103:15	362:21,23	79:11,13	238:9	97:13
128:25	363:1,3	79:15 84:5	244:11	98:16
133:3	372:13	99:5,7,23	245:3,19	113:18
136:25	374:6	105:20	310:23	128:24
147:18	<b>recorded</b>	158:3	<b>regularly</b>	135:21
150:9	10:5	185:23	116:1	137:22



**BRIAN J. SCULLY 1/12/2023**

143:16,18	266:8	150:11	142:13	145:23
232:9	<b>relayed</b>	151:12	361:20	157:9,13
233:1	251:6	171:23	362:13	157:16
239:10	<b>relaying</b>	176:20	368:8	159:6
243:9	180:23	194:3	369:21	161:9,21
285:13	251:12	207:14,17	370:3	162:21
326:15	<b>release</b>	208:20,23	371:7	163:19
371:15	253:24	209:1	<b>repeat</b> 19:3	164:12,22
<b>relation</b>	<b>released</b>	210:16	139:17	168:13,18
76:12	39:17	211:9	151:1	173:16
97:16	70:12	236:13,24	186:19	198:20
104:9	<b>releases</b>	237:7,13	197:5	200:3,7,10
<b>relation...</b>	129:7	246:12	223:17	200:19
47:18	<b>relevant</b>	247:3	249:2	201:13,23
55:25	135:19	248:12	291:13	203:16
65:23	160:4	250:23	<b>repeatedly</b>	204:6
67:25 68:3	189:10	251:11,21	245:11	205:11
76:9 79:9	191:12,15	259:1	247:11	209:16
80:9	192:20	272:17,21	<b>rephrase</b>	210:11
102:16	235:5	283:3	257:11	213:17
121:13,20	314:14	284:12	<b>reply</b> 282:18	214:12
148:21	315:2,14	285:11,12	<b>replying</b>	215:12,15
149:8,10	<b>reliable</b>	285:18	296:6	216:2,9
187:8	319:8	286:12	<b>report</b> 9:8	217:8,17
240:3	<b>rely</b> 13:2	351:21	9:12 21:13	225:1,10
310:16	<b>remain</b> 51:15	356:1	40:12 47:3	226:8
313:18	317:25	372:3	56:13	228:3,6
369:9,15	364:19	<b>remembering</b>	64:13	229:18,19
<b>relation...</b>	<b>remained</b>	241:19	68:18	231:2
238:17,20	51:13	306:16	69:20	256:13
239:24	<b>remarks</b>	<b>remembers</b>	70:12	264:24
240:16	337:2	248:4	71:18 72:2	280:8
241:14	<b>remember</b>	<b>reminder</b>	94:21	283:20
<b>relation...</b>	28:21 30:2	29:24	96:23	284:13
44:5 46:13	30:8,8	60:16	105:12	285:1,8
46:19,20	33:11,25	260:7	106:4	288:5,10
120:3	34:4 35:19	<b>remove</b>	117:23	289:19
131:20,23	35:20,25	283:14	118:13	297:5
215:25	36:1 37:15	<b>removed</b>	122:3	298:4
241:8,10	39:24 55:2	229:9	123:11	300:2,25
304:1	62:13	<b>render</b> 377:9	127:17	301:6
<b>relatively</b>	70:24	<b>Renée</b> 54:5	129:25	302:3
176:10	71:13	70:5,20	138:25	304:12
177:18,19	86:23	72:17	140:3,3	321:6
<b>relay</b> 164:13	87:19 95:3	116:22,25	141:1,3,15	328:11,17
220:21	98:2	117:6	141:15	328:20,22
221:18,21	104:14	134:22	142:18,23	329:22
222:16	116:11	136:6,9	143:2,21	335:15
265:14,21	124:6,11	139:7,9,23	144:7,11	352:20

**LEXITAS LEGAL**

**BRIAN J. SCULLY 1/12/2023**

364:15,17 <b>reported</b> 1:23 68:11 68:22 119:2 120:24 130:5,6,9 160:9,19 163:20,25 164:10 165:2 199:11 219:22 366:14 <b>reporter</b> 2:3 2:4,5,6,7 11:9 12:21 47:9 138:19 168:14 196:7 209:4 223:22 372:14,21 372:25 373:3 374:1,3 <b>reporter's</b> 10:14 <b>reporting</b> 8:5 16:22 23:25 26:10,11 26:14,16 27:8 36:8 39:20 40:6 40:24 41:14 44:9 46:14 47:19 50:24 52:17 53:9 63:23 64:23 66:3 66:16 68:8 68:14 71:25 74:24 79:11,13	79:17,20 79:25 81:2 81:3,20 82:10,11 82:22 106:21 114:8 116:1 118:2,15 119:8,12 120:5,8,21 121:1,5 159:13 161:5 163:9 173:13 193:10 198:21 201:2,25 202:13,19 204:8,18 205:6,22 206:24 207:2 208:10,15 210:2,7,12 210:25 212:9 228:14 235:4 238:25 243:10 257:4 259:13 263:8,15 278:3 279:4 282:7,14 282:25 283:4 293:5 300:19 306:3,10 320:25 326:10 363:13,15 363:20 364:8 <b>reports</b> 40:7	40:21 46:15 56:12 106:23 107:2,24 112:25 113:1,7,18 115:14,17 122:17 123:4 134:14,25 137:10,11 137:14 149:14 157:3,6 165:23 166:1 173:24 176:7,22 177:10 178:12,23 179:4 182:8 193:2 199:13 202:25 203:9 208:10,16 208:25 210:21 212:1 214:2 215:9,19 216:12 223:11 231:4 238:22 242:8,11 262:25 264:23 266:6,14 311:20 325:23 326:11 <b>repost</b> 347:11 <b>represent</b> 10:18 11:7 <b>represen...</b>	178:10 267:9 305:9 <b>represen...</b> 29:11 111:16 112:21 181:1 267:7 <b>reputati...</b> 340:23 341:3,5,11 341:12,18 342:15,25 <b>request</b> 45:7 277:2,14 320:18 337:17 372:18 <b>requested</b> 247:14 303:9 <b>requesting</b> 276:12 <b>requests</b> 191:13,16 192:21 233:2 337:22 <b>requirement</b> 115:24 227:8 <b>requirem...</b> 155:19 <b>requires</b> 320:20 <b>research</b> 44:6,9 46:11,16 46:17 47:3 47:6,9,19 48:22 49:23 50:1 73:12 144:17 145:20 187:13,16 195:10 196:14	209:18 221:17 326:10 <b>researchers</b> 143:14,17 145:22 325:23 <b>researching</b> 325:21 <b>resending</b> 346:24 <b>reserve</b> 11:2 <b>resilience</b> 16:5,8 42:23 45:25 118:2 131:4 303:22 315:24 324:10 332:1 343:3,21 347:20 358:2,5,8 <b>resilience-</b> 315:11 <b>resilien...</b> 316:3 <b>resilien...</b> 240:14 323:21 346:20 359:7 <b>resource</b> 62:19 63:8 166:11 173:23 <b>resourced</b> 57:9 <b>resources</b> 87:2,8 357:11 359:4 367:13 <b>respect</b> 40:16 93:15,19 142:15
---	--	---	--	--

**LEXITAS LEGAL**

**BRIAN J. SCULLY 1/12/2023**

<b>respond</b> 13:11, 23 93:20 176:6 199:22 223:10 293:16, 21 371:2	<b>responses</b> 6:23 176:14 188:22 189:14 190:19 193:23 194:5 226:12 231:17 242:15 293:24 353:2	261:17 <b>returns</b> 18:24 176:19 <b>review</b> 43:5 165:19 174:22 189:17 201:3 321:6, 14 321:16 <b>reviewed</b> 189:15, 20 194:2, 7, 12 207:10, 13 <b>reviewing</b> 207:14 <b>reviews</b> 25:18 <b>rhetoric</b> 126:22 <b>Richard</b> 161:4 350:11 <b>right</b> 11:2 14:6 15:15 18:6 19:13 20:15, 19 29:12 31:13, 24 43:11 44:13 48:7 50:14 51:21 57:22 59:7 59:22 60:2 60:19, 24 61:24 63:10, 15 63:17, 21 68:5 70:15 70:22 78:24 81:14 82:8 85:2 88:9 89:22 91:15, 18 91:20 93:8 96:19, 24	101:11 102:14 105:14 109:18 110:5, 7, 9 110:12, 15 110:19 111:3, 23 112:16 116:4 118:8 120:19 122:4, 7 123:18 125:10 137:15 140:10 141:4, 4 146:7 147:10 148:18 157:17 159:14, 15 161:2, 11 162:10, 19 162:25 163:3, 11 164:14 167:18 170:21 173:11, 17 176:7 177:5 179:20 181:6 183:23 189:12, 25 190:25, 25 191:6, 22 192:13 193:4 196:11 198:17, 18 199:23 200:4 202:5 207:2 208:1 211:1, 23	212:11 214:19 217:5, 9 218:13 219:6 223:14 226:2, 15 226:20 227:15 228:6, 10 228:17, 25 229:19, 24 230:2, 9, 14 230:18 231:2, 6 232:5, 11 233:14, 20 234:1, 6 237:11 241:7, 25 244:14 248:25 250:13, 24 251:4, 9 252:10 253:20, 22 253:25 254:4, 8, 13 256:5, 10 259:22 261:7 262:14 263:2, 21 264:24 272:2 273:10, 16 274:15 275:8, 13 275:23 280:25 281:19 283:17 287:6 288:3, 18 289:3, 5, 9 289:15 290:19, 20 291:22 292:19
<b>responded</b> 176:10 180:3 199:15 200:9 209:15 219:8 292:24	<b>responsi...</b> 90:14 289:17 353:20 <b>responsi...</b> 239:17 <b>responsible</b> 60:10 63:10, 12 115:25 169:22 175:20 343:17 <b>responsive</b> 176:21, 23 178:10 293:20, 23 331:20, 25 <b>rest</b> 134:23 186:1 282:17 349:10 <b>restrict</b> 132:13 <b>restricted</b> 95:16 <b>restrict...</b> 264:5 <b>restrictive</b> 132:18 <b>result</b> 96:6 <b>results</b> 13:6 <b>return</b> 19:16 375:19 <b>returned</b> 165:16			
<b>responding</b> 5:19 179:15 190:10 233:1 292:3, 5				
<b>responds</b> 176:2 206:1 224:17 226:14, 17 232:7 287:17 308:6 317:21				
<b>response</b> 9:16 43:24 107:15 133:7 147:9 165:7 177:23 191:12, 16 192:21 205:19 219:14 220:12 233:23 243:7 247:12 250:25 251:5 282:24				

**BRIAN J. SCULLY 1/12/2023**

293:25	327:15	100:14	23:19	167:2
294:11	341:18	129:20	58:17	<b>safety</b>
295:6,15	343:17	147:7,15	118:24	289:10,13
296:4,8	<b>risks</b> 16:15	149:20	138:10	289:13,14
298:10	56:17	150:15	172:17	<b>Salahuddin</b>
299:8,13	154:5	151:7,9,9	189:24	218:2
300:6,13	269:20,25	167:21,24	265:5	<b>Saleela</b>
300:15	270:8	168:10	291:24	218:2
301:12,15	309:5	171:17	348:14	<b>sat</b> 133:21
305:21	316:10	182:4,20	366:4,24	<b>Saturday</b>
306:21	323:7	239:17	367:22	173:17,18
308:19,23	332:2	240:2	<b>RPR</b> 1:23	173:19
311:25	342:21,25	278:10	374:18	176:1,1,11
312:5,16	343:20	303:22	<b>rules</b> 12:18	<b>Sauer</b> 3:3
313:2,11	354:21	305:17	126:18	5:3 10:19
316:15	355:24,25	311:24	152:4,13	10:19
328:25,25	356:2,7	313:21	155:16	11:15 14:2
330:16,25	358:4,23	316:13	260:10,14	14:17,23
331:21	<b>Rob</b> 43:20,23	317:11,18	<b>rumor</b> 290:13	23:3 34:22
339:5	166:17,18	345:10	290:19	35:8,13
342:16	167:1	371:1	291:12	53:2 69:9
344:19	179:18	<b>roll</b> 142:15	<b>rumors</b>	69:13
346:2,13	184:14	<b>Roman</b> 73:7	247:20	71:22 80:6
347:17	191:25	141:16	290:22	83:1,7,14
348:8,25	276:20	<b>room</b> 10:22	<b>run</b> 62:8	87:18 91:3
353:3	311:11,12	119:25	279:13	92:6 93:3
355:4,14	311:14,24	263:17,18	280:11,23	95:22
357:3	312:8,21	263:22,25	342:10,11	108:22
359:20	326:5,20	264:1,14	<b>running</b>	122:23
360:5,12	350:5	267:7,22	60:10	125:13
361:1,20	<b>Robert</b>	267:23,25	81:23	126:7
361:23	192:12	268:3	266:2	138:16,24
362:2,9	<b>robust</b>	<b>Rose</b> 308:10	312:21	139:4
368:15	265:25	308:11	<b>runs</b> 148:4	145:4,9
370:5,23	<b>Robyn</b> 10:15	<b>Roth</b> 7:4	267:17	148:9
<b>rigorous</b>	<b>Rodney</b> 32:17	238:1,2	342:6	151:3,4
222:4	33:9	244:3,9	356:1	152:25
<b>ring</b> 126:1	<b>role</b> 18:25	246:17	<b>Russia</b> 325:7	153:9
197:16	19:4 23:24	247:6	<b>Russian/...</b>	156:3,5,12
213:24	25:7,10,13	248:4	325:11	156:16
247:9	25:14	289:5	<b>Russians</b>	172:22,24
284:14	42:24	<b>roughly</b>	324:1	181:5,9
294:22	55:18,22	148:17		183:1,17
<b>risk</b> 11:22	59:2 62:17	<b>rounds</b> 286:7	<b>S</b>	185:8,11
44:14,16	62:18,21	287:1	<b>S</b> 3:1 4:1	190:15
56:20	62:22 63:3	<b>route</b> 268:25	5:1,6 6:1	191:2
236:6	63:7,13	<b>routed</b>	7:1 8:1	194:16,19
308:25	64:12	268:18	9:1 10:1	194:22
309:6	83:19,21	<b>routing</b>	<b>S-c-h-a-u-l</b>	195:2

**BRIAN J. SCULLY 1/12/2023**

196:2	344:12	338:16	225:4, 8	331:16, 22
197:3	345:13, 22	341:15, 17	229:20	332:10, 16
198:25	349:17, 20	348:19, 21	230:4	334:1
199:5	349:24	352:3	231:5	335:19, 23
204:21	350:1	368:13	232:7, 7	336:3, 14
205:1	352:15	371:7	244:9, 10	337:23
209:6, 13	354:14	<b>says</b> 73:8	246:18	338:14, 20
212:3, 13	359:15	88:12	247:6	344:5, 6
212:19, 22	362:20	89:19 91:4	250:20	350:8, 11
213:2, 9	363:2, 5, 8	91:11, 12	251:20	354:8, 20
215:4	364:13	94:21	253:23	355:9, 15
227:1, 11	365:12	95:18 96:5	254:6, 7, 10	357:6
227:21, 24	368:5	96:13 97:4	256:7	364:17
228:1, 19	369:19	97:12	260:6	366:1, 3
230:21	371:12	98:25	269:20	368:21, 25
231:20, 22	372:5, 14	107:14	270:16	369:5
231:24	372:16	108:10	272:9, 15	370:12, 15
232:2	<b>sausage</b> 85:7	109:6, 16	275:24	370:17, 21
242:20, 25	<b>saw</b> 12:24	109:19, 24	280:17	370:24
243:1, 24	116:2	110:7	281:8, 16	<b>SCHAU</b> 4:3
244:22	215:12	111:11	282:21, 25	<b>Schaul</b> 43:20
249:14, 17	293:12	117:24	283:10, 13	43:23
249:21, 24	319:25	118:14	284:23	46:10
252:3, 9, 13	324:5, 5, 6	122:11	285:7	166:18
252:22, 25	336:1	125:21, 25	287:3	167:2
253:3, 6, 10	356:18	126:17, 21	289:1, 21	179:18
253:13	<b>saying</b> 27:1	142:8	292:8	184:14
255:18	27:2 34:1	144:16	295:14	191:25
258:9	91:16	145:25	297:24	192:12
262:6	152:18	146:13	299:6, 11	276:20
271:14, 18	199:20, 22	147:2, 2, 11	299:16	326:5, 20
273:3	203:10	150:8	300:4, 11	350:5
276:1, 4, 11	223:13	158:8	300:15	<b>schedule</b>
277:15, 18	248:13	175:24	304:6, 7, 17	174:8
277:23	254:22	176:2	305:17, 22	<b>scorecard</b>
301:22	282:4	177:6	307:14	286:6, 11
302:9, 12	284:25	191:9	308:14, 18	288:3, 21
304:23	286:4	192:8	311:22	340:4, 8
306:20, 24	287:18, 24	195:13, 16	312:1, 15	<b>Scott</b> 3:4
309:22	292:25	195:21	312:25	10:22
316:21	294:8	196:5	314:11	82:23
318:24	296:6	197:17	316:12	319:5
319:2, 17	299:25	199:11	317:22	349:22
328:6	303:4	204:10, 11	320:2, 15	<b>screen</b> 14:10
334:23	307:3	206:20, 23	321:4, 15	14:10, 18
335:2, 7, 10	308:6	208:9, 13	321:24	15:3, 4
335:14	309:4	210:6, 19	328:21, 25	42:21
341:9	315:6	217:10	330:2, 13	69:14 72:8
344:8, 11	324:2	223:4	330:17	78:19 88:1

**LEXITAS LEGAL**

**BRIAN J. SCULLY 1/12/2023**

90:22	72:10	155:11	327:14,14	136:8,14
105:8,9	160:21	186:18	341:20	141:24,24
107:11,12	198:13	188:18	343:4,7,17	147:19,21
117:23	203:15	202:7	343:18	178:11
124:4	205:4	214:16	355:23,24	187:22
138:17	207:20	231:19,21	356:1,6	195:18
156:18	214:15	254:10	<b>sector's</b>	201:25
191:4	222:23	273:15	341:21	235:15,17
198:24	223:10,15	277:22	<b>sectors</b> 60:5	235:24
199:2	244:5	280:7,15	60:8	244:13,14
206:14,16	249:4	285:5,7	322:16	245:3,17
209:3	281:2	300:17	338:25	248:19
212:15	296:10	304:7	355:12	264:9
213:4,10	299:11	305:15	<b>secure</b> 298:3	267:13
215:2	320:1,14	307:6	298:4	270:12
222:21	344:4	345:16	<b>Securing</b>	294:9,13
225:5	<b>Scully</b> 1:14	346:10	47:8	295:11
227:20	2:1 5:2,8	352:3,17	<b>security</b> 4:7	296:21
252:8	6:3 7:3	354:4	4:13 5:19	305:6
281:7	8:3 9:3,16	355:9	9:22 11:5	320:3
306:25	10:5 11:12	357:5	11:23	321:5,14
319:19,25	11:16,18	<b>Secretaries</b>	15:24,24	321:16
328:8	83:15	50:8	20:5 25:6	327:16
335:11	188:21	103:14	26:13 33:1	332:25
345:19	191:21	<b>secretary</b>	33:3,15	336:7
363:9	209:14	204:6	35:6 50:6	342:2,5
364:14	219:4	205:12	52:12	344:19
368:10	251:7	206:5,15	55:23 56:5	352:24
369:20	253:14	206:19	59:7,10	353:6
<b>screwy</b> 209:3	269:21	207:4	61:7 62:24	359:18
<b>scroll</b> 87:23	372:12	214:13,18	63:20	360:3,25
105:7	373:8,11	225:1,18	64:20	363:12
108:24	375:12	304:15	67:14,21	<b>security...</b>
125:10	376:2	311:17,17	71:8,9,15	234:24
157:11	377:5,20	311:21	71:17,19	<b>see</b> 14:10,15
192:5	<b>search</b>	<b>secretary's</b>	76:25	14:17,21
195:9	192:20	101:18	79:14,17	14:22 15:4
197:10	222:4	311:19	79:21 80:1	15:16 18:6
201:17	<b>searched</b>	<b>section</b>	80:2 90:10	27:2 30:21
206:4	188:25	108:11	90:15 96:8	41:11 62:9
214:7	276:18	109:2	101:14,21	69:14 72:7
216:25	277:1	125:18	110:18	73:7,14
224:6,21	<b>searches</b>	193:25	112:6,11	78:22 83:1
244:8	144:18	281:5	113:12	87:25 88:1
245:23	<b>sec</b> 190:24	<b>sector</b> 16:20	119:10,21	88:8,15
282:16	<b>second</b> 35:21	18:12 44:8	127:15	91:10,12
285:15,25	82:23	47:12 60:4	128:24	97:8 98:20
302:23	98:23	60:5 308:3	129:11,24	99:2,3
<b>scrolling</b>	138:22	314:8	135:25	105:7,11

**BRIAN J. SCULLY 1/12/2023**

105:15	246:4,24	27:15 40:8	199:6	<b>sentence</b>
106:17	247:22	40:14,20	205:14,14	73:14
107:15	249:8	41:5,13	271:24	78:24
109:3	250:6,6,14	47:21	299:10	95:18,19
117:23	250:18	52:17	<b>senior</b> 4:4	96:1,5,12
118:3	253:8,14	82:15 83:4	22:12	96:20 97:4
122:14	259:9	114:12	129:22,23	109:11
123:12	261:3	194:4	251:17	118:4
125:3,17	269:7	235:8	305:5	122:10
125:20	270:18	258:13	360:17	125:21
141:25	271:23	279:4	<b>sense</b> 49:8	142:8
144:20	272:11	291:6	56:3 63:23	147:1,11
146:4,8,24	278:7	371:4	74:9	150:7
150:4	279:9	<b>seen</b> 20:20	120:23	207:5
152:5	286:3,7	50:23	136:11	246:17
154:19	287:3	124:18	152:12	247:6,19
156:23	289:7	244:5	268:14	250:5
157:6	296:9,12	259:8	290:16	280:9
163:10	297:12	321:16,18	369:12	287:2
165:19	298:4,22	363:22,23	<b>sensitive</b>	334:1
166:21,23	298:25	<b>semester</b>	352:4,5	355:8
170:4	300:2	170:15	<b>sent</b> 66:5,25	371:5
173:20	302:5,13	<b>senate</b>	67:7 69:10	<b>sentences</b>
176:3	302:15	197:16	106:13	90:14,25
191:9,17	304:10	<b>send</b> 106:8,9	121:4	<b>separate</b>
192:6	307:5,17	107:2	134:13,17	37:3 155:5
194:10	308:7	109:17	135:3	180:13
195:6	310:3,6	119:23	168:16	267:23
198:18	319:23	120:1,15	180:8	<b>separately</b>
199:1,16	320:5,6,21	131:15,17	190:6	129:3
201:22,25	320:22	210:2	193:6,9,12	<b>separation</b>
202:8	321:10,11	212:13,18	193:15	108:21
203:19	322:3	318:17	199:19	<b>September</b>
204:7	328:14	<b>sending</b>	201:24	18:23
205:22	330:11	66:25	202:3,7	19:13
206:5,11	334:5	134:24	203:17	20:24
206:15	335:17	157:3	212:22	21:20
208:7	336:17	180:14	214:14,18	24:11
213:3,10	338:2	193:21	217:19	28:24
213:16,21	340:6,16	211:21,24	226:13	31:12
214:12,14	346:10	211:25	230:5,11	36:10,13
214:24	350:6,9,17	242:7	265:3	38:24 39:5
215:1	354:8	252:3	284:24	41:8 282:3
222:1,21	357:11	295:3	286:3	283:9
223:8	360:22	307:2	288:17	364:15,25
225:2	361:6	345:13	294:2	<b>sequential</b>
228:2	368:16	368:14	351:19	170:5
232:6	369:22	<b>sends</b> 176:19	352:17	<b>series</b>
244:1,23	<b>seeing</b> 27:12	198:19	366:12	309:25

**BRIAN J. SCULLY 1/12/2023**

310:10	<b>seven</b> 233:21	328:8	<b>shifted</b>	372:9
<b>serve</b> 60:7	245:15	329:10	113:15	375:17
70:17	<b>shaking</b> 13:3	335:11	<b>shifts</b> 166:9	<b>signature</b>
109:6	<b>share</b> 14:10	345:19	166:13,14	373:7,19
189:23	14:10,18	363:10	174:13,21	375:14,17
<b>served</b> 19:8	15:3,4	364:15	174:25	375:20
147:7	17:7 25:19	366:16	193:9,11	376:25
367:3	36:9 40:5	368:10	<b>short</b> 104:17	<b>signed</b>
<b>serves</b> 366:3	40:10,17	369:20	151:18	157:18
366:23	40:20 41:1	<b>shared</b> 74:8	310:15	373:16
<b>service</b>	41:12	74:9 80:11	<b>shorthand</b>	<b>significant</b>
144:24	45:24,25	84:11,19	2:3,5	126:24
242:5	59:3 69:15	84:21	20:12	128:6
260:18	72:8 74:1	121:7,8,21	374:1	153:4
<b>services</b>	74:4,6	141:6	<b>shortly</b>	<b>signoff</b>
341:22,25	78:19 88:1	161:11	246:2	299:8
343:1,4,11	90:22	205:24	<b>shot</b> 206:16	<b>Silver</b> 312:8
343:14,18	105:8,9	213:6	225:6	<b>Silvers</b>
343:22,24	107:12	258:19	281:7	311:11,12
355:23	117:23	<b>shares</b>	<b>show</b> 176:17	311:14,24
356:4,5,13	138:17	196:23	190:16	<b>similar</b>
<b>serving</b> 20:6	156:18	<b>sharing</b> 17:9	242:14	52:24
63:13	160:3,15	59:15,25	243:6	54:17
147:15	160:16,17	60:4,6,17	<b>showed</b> 280:4	93:18
163:18	163:11	60:22	<b>showing</b> 14:3	100:3
367:14,22	164:17	78:21 79:5	160:5	134:23
<b>set</b> 6:24	191:5	80:10	227:12	136:19
16:3 21:9	199:2	121:24	252:15,18	139:12
47:20 58:1	206:14	147:6,7,15	255:14	140:6,25
61:4 63:14	211:11	147:15	279:10	238:16
68:16 88:9	212:15	148:5	342:17,19	243:20
103:8	213:4,11	164:3	<b>shown</b> 229:7	296:23
165:17	215:2	235:6	<b>shows</b> 157:2	314:19
179:7,17	222:22	260:4	205:11	<b>simultan...</b>
181:7	234:18,20	263:4	269:11	196:23
253:8	235:5,12	264:11	<b>shredded</b>	<b>simultan...</b>
256:3	252:8	284:12	339:11	169:24
262:16	258:1,20	288:24	<b>side</b> 15:15	183:21
312:3	259:14,24	298:7	28:1 38:7	185:16
364:25	260:10,25	<b>sheet</b> 43:2	40:4 43:24	195:23
374:13	285:1	373:16	44:18 54:4	197:8
<b>sets</b> 39:18	287:5	376:1	127:23	200:2
303:14,23	288:23	<b>sheets</b>	236:25	<b>Sincerely</b>
<b>setting</b>	294:9	375:14,17	237:2	375:22
65:20	296:8,11	375:19	310:4	<b>single</b>
99:20	299:3	<b>shift</b> 174:15	315:19	363:15,19
159:2	306:25	175:3	<b>sides</b> 40:3	<b>SIO</b> 97:5
<b>settle</b> 62:23	311:24	180:15	238:20	104:4,12
<b>setup</b> 119:25	319:19,25	193:15,20	<b>sign</b> 11:2	104:15,17

**LEXITAS LEGAL**



**BRIAN J. SCULLY 1/12/2023**

181:14,17	253:16	168:7	317:13	<b>sorry</b> 16:9
182:19	350:4	172:5,18	318:4	19:2 23:5
183:15,22	<b>so-called</b>	180:15	326:14,24	29:9 30:9
183:23	126:4	189:24	327:3,9,18	31:9 37:10
187:2,3,3	254:17	192:2	333:16	40:2 47:9
187:4,6	<b>social</b> 17:4	193:3,9	339:10,23	55:1 60:12
195:15,24	17:8,10,12	200:20	340:4,5,8	66:14,23
196:24	17:16	208:23	341:13,16	67:3 70:7
197:8	18:16,21	210:12	346:25	76:20 84:5
<b>sir</b> 15:5	20:8 21:1	214:3	350:15,21	86:6,7
153:11	21:5,23	220:4,6,25	350:21	90:21 91:8
<b>sit</b> 130:8	23:20 24:2	221:20	351:2,6,13	95:25
<b>sitting</b>	24:5,10,13	222:16	351:24	100:15
263:17	27:1,22	223:20	352:11	104:1
<b>situation</b>	38:13 39:8	228:9	356:19,19	113:3
161:8	57:21	229:4,8	357:8,15	114:16
223:2	58:17 59:3	232:8,25	357:19,21	122:7
228:13	64:2 66:5	233:18,22	363:16	125:8,12
344:23	66:16,25	235:13	364:21	125:15
<b>situational</b>	67:17 68:8	237:3	365:2	138:2
155:7	73:11,18	239:11,21	366:2,5,25	139:17
267:17,24	78:21 79:6	241:6	<b>society</b>	143:16
268:2	93:21 94:7	242:16	16:19	145:6,7,10
325:24	94:13	244:18	73:11	147:2
326:1	107:20	245:4,16	105:13	150:25
<b>six</b> 73:7,7	108:2	246:23	109:12,17	151:22
126:14	109:13	247:25	354:22	155:3
270:16	114:24	256:14	<b>solving</b>	163:13,15
331:1	118:25	257:17	65:25	164:13
337:25	120:22	258:2,5,12	<b>somebody</b>	166:17
338:6	122:18	258:13	62:22	167:20
349:23	123:5,17	259:4	102:2	168:4
<b>size</b> 105:9	126:18	261:3	133:19	171:23
<b>sizes</b> 357:9	127:5	263:24	135:4	173:8
<b>skip</b> 334:24	129:12	265:17,22	168:6	178:1
<b>skipping</b>	131:20	266:9	174:12	186:2,18
141:15	132:1,12	268:23	224:14	195:4
298:19	132:17	269:1	227:5	196:8
<b>slash</b> 28:9	134:4	274:5,8	263:13	197:5
<b>slightly</b>	138:11	277:9	333:8,10	198:22,25
91:14	144:4,24	278:7,13	358:11	214:9,15
<b>slowly</b>	146:3	286:19,23	<b>somewhat</b>	218:4,9,14
345:18	151:8	290:12,25	15:13	221:8
<b>small</b> 122:19	152:18	291:25	105:10	222:11
193:25	153:15	293:5,6	352:4	223:15,17
<b>Smoke</b> 281:16	157:9	296:16	<b>Sonoma</b> 163:9	225:22,23
<b>smoothly</b>	163:19	300:18	<b>soon</b> 14:15	225:25
15:2	164:11,13	305:18	198:14	226:1,1,4
<b>Snell</b> 28:8	165:3	314:21	335:9	227:19

**LEXITAS LEGAL**

**BRIAN J. SCULLY 1/12/2023**

232:3, 14	100:9	279:15	<b>specific</b>	133:22
232:23	102:11	338:1	27:19, 20	135:9
233:18	114:21	<b>speak</b> 14:20	37:17, 25	149:9
241:3	115:7	27:8 36:2	38:11	150:3
243:4	123:24	42:5 56:2	39:24	207:17
249:1, 21	130:16, 16	58:3 61:21	56:15, 24	235:9
252:13	131:1, 7	64:16	74:6, 14, 16	237:1, 7
253:9	151:20	67:13	75:3 90:12	242:6
257:11	152:4	87:22	116:12	245:17
262:3	179:12	115:16	120:10	246:9
268:12	206:25	131:16	129:9	254:8
269:10	220:22	149:11	133:21	256:17
273:9	234:20	161:24	143:24	259:15
274:22	286:21	177:20	216:23	275:17
279:22	329:14	207:3	220:12	276:24
280:14	345:12	243:12	236:10	282:11
281:6	368:18	367:18	237:16, 21	283:24
282:1	<b>sorts</b> 20:25	<b>speaking</b>	240:8	284:17
284:9	25:21	15:22 16:7	241:19	297:1
291:13	26:25	24:24 27:7	242:3	301:6
292:12	27:16	27:10, 17	247:13	341:16
293:11	40:13	33:21 36:6	255:4	<b>specificity</b>
297:17, 17	129:1	37:19, 21	258:24	211:13
297:20	147:24	65:5 74:2	268:8, 14	<b>specifics</b>
299:23	304:4	79:19	272:22	37:20
302:6	342:8, 12	83:18 94:4	273:12, 24	39:24
303:3	343:9	107:5	278:14	80:10
305:15	356:9	119:14	282:13	107:21
307:23	<b>sound</b> 279:25	128:2, 7	285:12, 12	141:9
311:1	334:21	143:13	285:24	181:20
314:1	<b>sounded</b>	177:17	290:5, 9	247:4
318:21, 22	54:16	215:11, 22	294:18	251:25
320:1	<b>sounds</b> 96:14	220:14	303:7	286:17
325:15	160:13	235:1	304:13, 25	<b>specify</b>
327:8	207:18	257:6	305:20	115:11
330:21	308:21	258:21	336:6	200:13
334:23	364:1	263:10, 12	341:8	<b>speculate</b>
344:7	<b>source</b> 16:22	264:25	345:25	91:23 97:2
347:12	42:16	304:2	<b>specific...</b>	216:6
351:23	123:14	305:10	37:16	231:14
361:17	274:5	309:4	65:24 74:3	272:15
363:5	279:6, 11	325:20	84:6 99:6	<b>speculating</b>
368:13	325:21	340:10	103:20	68:23
369:23	326:8, 9	357:18	105:24	266:10
371:10	<b>sources</b> 24:4	358:7	113:10, 14	<b>speculation</b>
<b>sort</b> 18:3	123:9	<b>special</b> 4:4	113:21	71:21 72:4
30:23	329:4	320:19	118:19	87:17 97:1
47:15	357:22	<b>Specialist</b>	121:19	98:12
99:20	<b>space</b> 25:6	4:20	124:9	111:9

**BRIAN J. SCULLY 1/12/2023**

115:10	<b>spoke</b> 78:4	276:20	89:6	100:7
118:17	334:21	<b>stage</b> 47:7	<b>Stamped</b> 6:5	101:25
122:22	<b>spoken</b> 307:3	174:2	6:14,21	104:18,22
142:7	<b>spot</b> 284:10	<b>stages</b> 241:9	7:9,10,13	117:5
149:18	348:25	<b>stakeholder</b>	7:18 8:5	142:2,25
178:16	<b>spread</b> 32:6	108:19	8:21,22	147:20
194:15	144:19	110:8	9:14,19,20	169:7,12
198:6	158:10	111:7,12	<b>stand</b> 270:14	169:15,20
201:5	<b>spreader</b>	<b>stakehol...</b>	307:19	169:25
202:16	126:3	16:13,19	308:15	170:11,14
204:13,24	<b>spreaders</b>	18:11,16	<b>standard</b>	170:15
231:11	125:23	20:9 44:15	66:18	172:8,11
244:21	<b>spreading</b>	97:7	180:5	172:11
273:2	114:23	105:13,22	187:13	182:7,13
283:22	124:24	108:11,15	200:25	182:24
294:17,24	160:8	108:25	372:18	185:16
298:12	207:8	109:3,5,7	<b>standing</b>	186:11,11
304:22	323:4	109:12	179:3	186:13,23
310:13	<b>spreads</b>	137:25	<b>standpoint</b>	188:2,5,8
316:20	323:11	147:10	46:22	195:11
324:25	<b>spreadsheet</b>	152:9	143:25	196:15,18
333:19	165:15,22	263:3	154:21	204:9,11
351:16	166:2,5,8	264:2	239:24	204:15,16
352:8	190:6,9	303:25	332:24	204:17
354:13	193:14	322:20	359:7	361:22
356:22	201:10,14	366:2	<b>stands</b> 59:16	362:3
358:15	<b>spring</b> 70:9	<b>stalled</b>	146:10	368:14
359:23	89:10	364:19	307:22	370:4
360:20	<b>stability</b>	<b>Stamos</b> 70:5	<b>Stanford</b>	<b>Stanford's</b>
361:14	339:7	70:14	46:23 48:2	134:10
<b>speech</b> 320:4	<b>staff</b> 16:2	72:17 76:9	48:18	<b>Starbird</b>
348:5	28:9 53:25	76:14,15	49:20	72:21
<b>speed</b> 275:22	54:6 57:8	77:8,17,22	50:22,22	87:25
<b>speed/pr...</b>	113:10,12	77:25 78:7	51:8,10,15	360:5
272:10	113:13	85:22,23	51:22 52:5	<b>start</b> 14:3
273:16	148:25,25	86:3,11,16	52:11 58:9	212:6
275:23	149:1	87:15 88:8	58:11	233:11
<b>spell</b> 32:20	171:8	98:7 99:10	70:14,21	244:8
155:3	330:19,22	99:16	70:21	<b>started</b> 12:2
167:5	331:1,11	101:2	72:16	24:17 32:2
279:23	333:8,13	111:22	74:18	76:17
<b>spelling</b>	<b>staffing</b>	116:20,24	76:14 78:4	88:24
373:4	173:23	117:2,5	78:5,8	89:13
<b>spend</b> 87:7	<b>Stafford</b>	136:9	80:17,21	117:1
<b>spent</b> 314:9	167:19	139:7	80:23 81:6	174:4,5,20
<b>spilling</b>	179:19	142:12	81:12,17	174:21
247:19	184:14	362:12	82:2 83:24	336:12
297:9,15	191:25	368:13,21	85:6 89:4	368:14
<b>split</b> 107:11	192:13	<b>Stamos's</b>	89:6,11,20	<b>starting</b>

**LEXITAS LEGAL**

**BRIAN J. SCULLY 1/12/2023**

12:5 18:6	377:1	<b>stead</b> 21:1	338:12	<b>subdivision</b>
98:3	<b>state's</b>	<b>stenogra...</b>	<b>string</b> 7:8	15:9
241:20	204:6	374:7	9:18	307:25
283:14	205:12	<b>step</b> 80:19	<b>strong</b> 96:7	<b>subject</b>
297:8	206:6,15	106:25	317:6	150:20
307:1	206:19	263:2	<b>structure</b>	152:22
323:24	214:13,18	347:10	339:8	153:19
<b>starts</b> 324:4	<b>state/local</b>	<b>steps</b> 16:14	<b>stuck</b> 188:1	217:15
<b>state</b> 1:5	24:1	123:12	<b>student</b>	246:21
10:6 11:16	<b>stated</b>	171:25	169:7	255:22
24:4 38:2	148:18	221:13	<b>students</b>	282:13
44:23 50:9	334:2	231:6,8	50:22,23	289:23
50:9 54:20	<b>statement</b>	295:4,19	51:15	297:11
54:23	21:12,13	298:3	89:20 90:1	361:5,16
57:18	218:18	302:17	97:5 370:4	<b>submitted</b>
58:23 60:1	219:21	304:13	<b>studies</b>	108:9,10
60:23 61:3	220:16	316:9	170:11	189:18
79:3 85:1	221:1,3,10	357:13	<b>study</b> 95:15	199:21
91:19	221:15,22	<b>stood</b> 60:7	<b>stuff</b> 15:3	200:4
93:15 96:6	221:24	80:20	53:17	243:13
96:16	222:2,6	104:9	64:13 96:3	<b>submitting</b>
101:10,18	253:20,21	325:5	115:3	105:22
101:19	253:24	362:12	116:3,8	<b>subscribe</b>
103:14	254:3,7,15	364:4	121:24	145:2
106:11	254:22	<b>stop</b> 266:19	166:13	377:11
148:5	314:19	<b>store</b> 281:9	169:15	<b>subsector</b>
149:15	<b>statements</b>	<b>stories</b>	177:21	59:15
164:8,14	127:21	124:19	184:4	60:15
204:17	219:18	<b>straight</b>	187:11	339:7
207:4,7	222:14	120:18	188:11	<b>subsidiary</b>
215:10	225:10	<b>strategic</b>	189:11	38:18
221:25	<b>states</b> 1:1	25:18 36:7	227:6	<b>substance</b>
223:4	10:9,25	36:8 37:22	234:20	377:8
225:2,19	41:12	235:3	238:17	<b>substantial</b>
246:1	45:19	<b>strategi...</b>	240:16	50:23
265:20	59:22	27:11	241:14	135:23
266:7	90:18 91:5	<b>strategy</b> 9:9	289:13	153:4
278:4,11	94:22 95:6	12:10	366:8	264:4
278:19	95:12,16	321:7	368:18	317:18
281:18	147:10	328:13,24	<b>sub-bullet</b>	<b>substant...</b>
296:17	223:25	329:2,8,11	354:22	136:1
297:2	275:7	<b>streamlined</b>	357:6	<b>suffice</b>
298:9	342:1	65:11,14	<b>subcommi...</b>	301:4
299:11,21	<b>stating</b>	<b>Street</b> 3:9	72:24,25	<b>suggested</b>
300:20	329:23	3:20 375:6	353:3,7	312:3
304:15	<b>statutory</b>	375:21	<b>subcommi...</b>	<b>suggesting</b>
369:3	61:20	<b>strengthen</b>	70:18	95:4
375:8	<b>stay</b> 107:12	336:16,20	<b>subcompo...</b>	286:20
376:3	173:3	<b>stressed</b>	118:1	<b>summarized</b>

**LEXITAS LEGAL**

**BRIAN J. SCULLY 1/12/2023**

74:13	<b>suppose</b>	187:2,4	362:19	170:19
<b>summary</b> 36:9	17:25	188:11,16	<b>surprised</b>	171:1,4
73:7 74:15	45:11	197:23	52:18 76:1	173:25
89:15	219:12	198:4	237:9	184:6,18
260:9,13	221:14	201:8	247:16	189:23
260:21,22	340:3	203:2	272:23	193:4,6
346:16	<b>supposedly</b>	207:10,12	296:23	213:15
<b>summer</b> 36:16	218:25	211:15,21	334:14	216:13
36:17 70:9	<b>suppressed</b>	218:7	<b>surprising</b>	241:21,24
86:4 97:6	320:19	219:9	273:10	265:11,14
117:1	<b>suppresses</b>	221:2	<b>suspect</b>	266:21
151:18	354:23	223:16,19	103:3	<b>switched</b>
170:9,10	<b>Supreme</b> 3:8	237:18,25	108:24	252:14
186:7,14	<b>Sur</b> 3:18	238:18	163:7	<b>sworn</b> 11:10
187:8,24	11:5	239:13	261:18	11:13
188:10	<b>sure</b> 11:18	240:6	289:16	<b>sync</b> 21:4
234:7	15:1 16:10	241:11	290:3	24:13
<b>Summit</b> 5:19	17:12	243:16	326:21	36:20 78:7
<b>super</b> 239:15	20:20	249:2	331:6	127:19,22
325:18	26:22 29:8	256:16	333:10	128:14
<b>supervision</b>	34:2 42:13	257:13,15	<b>swear</b> 11:9	132:4
374:9	52:14	259:20,23	<b>switchboard</b>	233:17
<b>supervisor</b>	54:24 56:1	261:8	16:24 17:1	238:9
22:13	57:2 60:14	265:2	168:10	244:17
140:22	61:4 62:5	267:2	263:15	245:14
141:11	63:1 65:1	269:10	366:3,23	246:7
<b>suppleme...</b>	65:15	271:17	367:15,22	247:2,11
276:13	66:12 67:3	273:19	<b>switchbo...</b>	255:3
277:2	68:25	286:25	131:16	260:5
<b>supply</b>	74:12 77:1	295:24	179:16	269:6,14
220:24	79:11,14	296:19	<b>switchbo...</b>	269:25
<b>support</b>	80:8 84:12	299:19	64:16	272:2
54:18	85:13 93:6	300:22,24	<b>switchbo...</b>	306:2,9
184:4	102:15	301:1	21:25 22:2	317:16
220:8	124:18	302:24	23:17,19	<b>synch</b> 178:25
301:9	132:9	303:10,25	23:24	238:6
307:17	135:2	305:11	62:17 63:3	<b>syncs</b> 132:5
322:2	140:21	306:15	63:7,17,20	<b>system</b> 96:8
325:3	149:7,12	316:25	64:7,9,12	158:20,24
331:3,14	151:1	331:8	118:21,22	159:4
337:11	152:2,9	337:6,7,20	118:24	181:23,25
<b>supported</b>	161:1	363:22	131:9,12	182:1,3,7
90:10	162:13	365:22	138:4,5,8	182:7
149:2	166:4	<b>surprise</b>	149:3,5,20	267:13
<b>supporting</b>	176:17,24	80:11	156:21	342:4
187:11	178:21	236:22	161:20	355:13,17
331:3	181:8,13	247:4	163:18	355:20
<b>supports</b>	184:7	252:1	166:1	<b>systems</b> 2:7
43:17,20	185:23	255:6	169:1	270:12

**BRIAN J. SCULLY 1/12/2023**

288:6	137:20	116:15	245:20	370:3
341:25	140:8	127:18	250:17	<b>talks</b> 44:19
342:11	141:2	128:3	259:13	78:20
374:20	142:14	133:21	263:7,21	90:14
	147:13	172:4,23	264:15	108:9
<b>T</b>	157:8	208:9	306:2	146:6
<b>T</b> 4:1 5:1,1	158:6	209:21,24	310:23	254:3
5:6 6:1,1	170:13	240:1,13	312:19	363:13
7:1,1 8:1	179:16	241:12,23	335:3	368:12,18
8:1 9:1,1	183:1	258:3	351:13	370:8
<b>table</b> 73:6	190:1,21	296:2	355:16	<b>tally</b> 349:23
232:17,18	219:20	306:14,14	360:11	<b>tangential</b>
232:18,19	221:13,23	311:7	362:5	13:13
<b>tactic</b>	231:8	325:22	368:19	<b>Tangle</b>
114:19	242:3	344:14,18	<b>talking</b>	144:18,22
236:11,21	261:2,12	349:6	28:24 31:2	144:23
246:11	275:5,11	356:18	31:11,17	145:2,13
255:7	276:1	357:10	41:7 45:14	146:7
273:11	277:14	359:4	47:10	<b>target</b> 57:16
<b>tactics</b> 41:5	313:14	<b>talked</b> 26:20	56:24	321:8
41:13	316:9	26:21,22	83:15	<b>targeted</b>
114:11,22	318:22	46:22,24	91:14	114:19
114:23	328:22	58:10 63:3	96:15	254:11
116:12	342:18	65:10,11	114:25	256:10,19
279:6	345:17	72:13 82:1	145:19	278:20
316:6	348:7	85:5,21	163:5	<b>targeting</b>
323:4	349:3	91:15	185:8	16:5 57:11
359:10	358:24	93:14	206:12,13	87:3 96:10
<b>take</b> 16:15	361:9	96:15	208:14,21	96:18
31:10,19	367:4	99:11	210:24	154:1
43:8 50:13	<b>takeaways</b>	100:16	217:12	331:17
57:24	141:8	121:17	237:14	<b>targets</b>
60:21 63:2	143:20	132:4	239:13	258:19
63:6 65:10	<b>taken</b> 177:13	140:21	240:21	<b>task</b> 12:5
80:19 81:9	178:6	142:21	242:6	118:1,7
81:10 85:9	288:11	147:22	243:10	130:2
89:10	304:13	157:22	244:25	271:6
94:12	374:4,7	161:13	245:1,21	312:2
96:22	375:12	171:21	246:13	330:15
103:7	376:4	173:22	256:12,17	348:13
106:25	<b>talk</b> 5:15	179:1	259:3	<b>tasked</b>
111:21	12:21	181:18	260:7	174:13,14
112:4,9	26:11 41:3	208:15	263:25	<b>tasks</b> 90:12
116:2	41:4 45:5	213:25	274:7,9	<b>team</b> 8:13,15
118:6,23	47:13 84:4	216:18,20	294:3,14	15:17,23
120:20	99:25	233:6,7	294:19,21	16:2,2,4
121:10	100:10	235:10	296:15,20	18:4,8
123:12	102:19	238:10	333:22	19:10
133:6	111:22	244:17	335:5	36:14

**LEXITAS LEGAL**

**BRIAN J. SCULLY 1/12/2023**

39:15	348:12,13	221:17	317:17	114:21
42:24	350:13	348:15	336:23	143:6,8
44:10	353:10,12	<b>tells</b> 280:10	345:8	210:17
75:20	353:13	340:5	373:13,14	219:13
102:3	358:24	<b>tended</b> 216:5	<b>text</b> 8:22	280:19
113:13	366:3,23	<b>tenth</b> 283:7	217:4	295:4
115:19,25	367:12	<b>term</b> 138:9,9	309:25	301:14
117:12	368:14	242:5	310:3	309:9
118:8,10	<b>team's</b>	293:20	312:1	345:12
118:15	342:23	<b>terminology</b>	316:11,12	<b>things</b> 16:3
131:18	<b>teammates</b>	127:13	317:21	25:4 26:25
143:22	308:7	<b>terms</b> 31:18	<b>texting</b>	27:11,17
159:14	<b>teams</b> 42:9	54:18	310:11	41:17 43:5
161:6	287:18	83:22	<b>texts</b> 310:10	44:3,18
166:9,12	288:1	154:4	<b>thank</b> 29:24	46:16
171:18,20	311:9	155:21	87:24	55:10 69:4
174:5	<b>tech</b> 279:12	166:10	88:14	71:4
180:7	279:14	184:6	183:10	113:16
188:25	<b>technical</b>	260:18	199:4	114:11,19
189:4,7	83:17,17	288:23	206:2	115:2
263:13,14	146:19	317:18	224:17	124:19
263:19	195:18	<b>terrorism</b>	227:21	129:1
278:25	<b>technically</b>	26:23	272:1	131:7
279:16	130:9	27:16	300:12	144:9
289:10	175:2	<b>test</b> 152:11	308:14	159:3
299:1	<b>technique</b>	154:7,10	367:3	168:14
303:20	115:4	154:17	<b>thanked</b> 89:9	174:9
305:18	<b>Technolo...</b>	<b>testified</b>	<b>thanks</b> 176:2	207:1
307:15	9:25	11:13	199:16	216:16
311:9	<b>technology</b>	150:10	200:10	235:11
312:2,3	286:16	156:22	277:15	238:23
318:11	<b>teleconf...</b>	192:25	292:25	254:8
320:11	332:13	193:8	295:3	256:8
325:10	334:2	245:11	299:21	258:19
326:5,7,21	<b>tell</b> 111:19	255:24	<b>theft</b> 76:25	260:6
326:23	118:22	276:19	<b>theirs</b> 67:15	264:18
330:21	158:13	309:10	301:11	268:25
331:5,6,10	198:14	360:24	<b>theme</b> 259:5	270:13,14
331:13,16	211:23	365:3	349:8	279:7
331:19,23	214:5	367:4	<b>themes</b> 256:8	284:2
335:20,25	215:11	<b>testify</b>	256:14,21	290:20
336:5,17	244:25	251:16	257:18	291:2,6
336:21	257:18	<b>testimony</b>	258:4,12	292:8
337:4,15	266:17,23	23:7 89:25	259:1	304:4
338:22	287:12	97:22	<b>theory</b> 154:8	306:13
343:19	334:16	118:23	154:10	316:7
344:22	349:1	119:6	<b>thereon</b>	325:23
346:16	<b>telling</b>	202:18	377:10	326:11
347:23	35:18	276:16	<b>thing</b> 88:9	333:24

**LEXITAS LEGAL**

**BRIAN J. SCULLY 1/12/2023**

334:16	125:6	255:24	371:25	<b>threats</b> 25:3
340:15	128:1,21	256:9,22	372:5,18	26:16,21
342:12	131:22	256:25	<b>thinking</b>	26:23
345:11	134:21	257:12	37:23	27:16
346:24	135:24	258:15,16	53:15 58:5	235:18,24
348:1,22	136:13	258:22	85:15 87:6	340:17
348:24	137:7,8,16	259:6,21	99:22	366:15
349:13	139:20	261:9	100:2	<b>three</b> 19:8
358:23	140:2,4,17	262:5,19	<b>third</b> 72:10	35:17,23
<b>think</b> 15:1	142:17	263:17,21	90:4	43:17,22
19:12	143:4,5,23	265:24	119:25	44:8 48:18
20:17	144:10	267:8	249:25	50:11
24:18	149:4	268:7,9,15	320:15	110:11
26:23	150:10	268:20,21	346:7	119:8,17
38:25 47:3	156:21	270:25	361:19	187:14
48:1,17	157:4	271:2,12	364:16	191:17
49:1 50:3	158:16	276:22	365:17	214:19,21
53:23,24	162:16,18	279:18,19	366:1	215:5
54:22 55:1	165:14	281:17	368:11	254:8
55:7,22,25	166:20,22	286:23	<b>third-party</b>	308:22
56:11,16	167:1	288:14	288:1	331:3
58:4,7,10	169:2	290:24	325:22	345:15
58:13 59:5	173:5	295:8,9	326:10	<b>throttled</b>
60:18	174:2,13	296:1	<b>thought</b>	320:19
65:13,17	175:10	298:14	56:14,20	<b>throw</b> 217:11
65:19,22	177:17	300:23	58:14	<b>Thursday</b>
66:7 71:1	180:4,20	301:3	100:1	1:15 157:2
72:15	181:3,18	305:8	116:3	<b>ticket</b>
74:15	182:16	306:1,8,12	145:7	144:16
80:14	187:3,3	306:12,17	159:13	146:2
81:19 82:5	192:5	307:22	160:4	158:10,18
82:8 83:15	194:7	311:4	161:5	161:15
84:14	197:14	314:6	227:25	162:19,22
87:11	198:16	315:5	232:14	199:13
88:24	204:16	317:5	252:17,17	<b>ticketing</b>
90:11	212:11	318:7	260:18	158:20,23
91:25 92:7	215:20	328:1	<b>thread</b> 81:5	159:4
92:12,13	220:5	329:11,13	81:10	181:22,25
93:18,24	222:3	329:17	<b>threat</b> 37:17	182:1,3,6
94:2 100:6	227:14	333:4,7,11	37:23 38:1	<b>tickets</b>
100:7,17	232:12	337:8	338:13	108:9,10
101:4,15	233:9,21	341:22	339:12	109:17
106:1,15	236:4	344:15	341:13	110:1
112:15	239:4	345:4	<b>threaten</b>	122:12
113:4,4	240:23	351:10	340:8	<b>tier</b> 106:18
117:7	245:22	353:19	<b>threatening</b>	107:14
119:15	250:20	357:24	235:20	<b>tiered</b>
124:14,15	251:7	365:3,21	<b>threatens</b>	144:15
124:16	252:13,15	369:10	340:11	<b>time</b> 10:4



**BRIAN J. SCULLY 1/12/2023**

22:15, 18	351:4, 4, 11	214:5	303:18	169:19
22:22	351:11	<b>tips@202...</b>	<b>tonight</b>	190:6, 8
28:24	352:4, 5	203:1	292:9, 11	228:9
30:17, 25	360:18	230:17	292:14, 15	229:3
34:24 35:2	362:22, 25	<b>tips@202...</b>	292:17, 18	287:4
41:7 46:3	372:12	202:8	<b>tool</b> 145:21	288:22
55:16	<b>timeframe</b>	204:2	<b>tools</b> 108:6	289:2, 21
70:12 78:8	31:1 36:10	205:13	155:21	<b>traction</b>
83:9, 12	39:10, 18	213:21	231:13	228:10
87:7 90:7	55:6 71:15	230:9, 14	<b>top</b> 15:7	229:4
100:25	85:10 86:8	<b>tips@202...</b>	83:4	<b>traditional</b>
105:2, 6	86:18	203:18	157:16	254:18
127:16	87:15, 21	<b>tips2202...</b>	163:6	<b>traffic</b>
139:10, 24	104:20	205:5	201:22	159:24
141:12	122:19	<b>title</b> 11:20	241:19	<b>transcribed</b>
142:23	129:20	15:19 29:5	289:19	12:20
158:17	170:24	29:9 32:24	299:14	<b>transcript</b>
164:25	177:7	32:25	338:13	5:7 6:2
169:4, 5, 8	227:2	129:19, 23	<b>topic</b> 13:13	7:2 8:2
169:24	285:19	289:11	181:6	9:2 13:7
180:22	293:7	311:16	312:12	368:12
181:4	327:25	335:19	<b>topics</b> 236:5	370:2
183:5, 8	337:14	<b>today</b> 11:3	248:9	372:15
186:24	<b>timeline</b>	13:3 14:8	274:15	374:5
209:8, 11	55:6, 8	20:13	308:22	375:16
218:1	98:20, 24	240:21	315:14	<b>transcri...</b>
220:1, 1, 9	178:8, 18	244:17	321:10	5:14, 18
249:11	179:11	245:11	<b>total</b> 180:20	373:14
255:10	<b>timelines</b>	276:16, 19	<b>touch</b> 59:6	<b>transiti...</b>
265:17	101:6	282:6	62:12, 12	330:14
271:12	176:19	283:11	101:13, 16	<b>transpar...</b>
276:6, 9	<b>times</b> 38:22	299:7	101:24	261:10
277:5	174:15, 15	334:9	102:1, 5, 25	<b>transparent</b>
287:19	174:16	364:22	112:6, 10	260:19
297:10	177:22	366:22	112:13	<b>Treasury</b>
300:17	201:10	<b>today's</b> 10:3	234:14, 21	343:16
302:21	230:20	253:20, 25	351:6	350:13, 19
303:1, 3	238:5	254:7	<b>track</b> 45:17	350:25
306:5	247:10	<b>Todd</b> 3:4	151:23, 24	351:22
314:9	255:6	10:22	152:17	352:5, 10
315:21	273:10	<b>Todd.sco...</b>	153:15	355:22
319:10, 13	351:9	3:14	165:22	356:15
323:23	<b>timestamps</b>	<b>told</b> 86:25	<b>tracked</b>	<b>trend</b> 40:5
324:9	293:2	215:15	144:2	315:8
327:25	<b>timing</b>	246:18	161:15	<b>trending</b>
331:4	177:20	267:3	<b>tracking</b>	231:6, 9
333:14	<b>tiny</b> 73:5	<b>tomorrow</b>	150:16	<b>trends</b> 41:13
334:5	<b>tips</b> 66:14	277:3, 12	158:10, 14	235:8
336:8	202:14	<b>ton</b> 238:23	165:15, 19	305:20, 24

**BRIAN J. SCULLY 1/12/2023**

306:7	347:16	290:10	283:8	223:11
314:14,18	357:25	291:11,19	288:18	226:14,19
314:21,23	358:5,9,17	<b>tweets</b>	289:9	230:7,12
315:1	359:8,11	159:17	291:1,19	248:24
323:3	<b>trying</b> 49:20	177:4	291:20	256:10
<b>triage</b>	54:18 91:8	226:19	293:15	259:6
107:15	91:23 93:7	292:9,14	298:23	268:9
<b>Trick</b> 213:8	94:4 97:3	292:16	299:6,20	271:11
<b>tried</b> 239:18	131:5	305:20	300:4,15	272:9
<b>tries</b> 344:22	135:23	<b>twice</b> 333:8	301:5,10	279:18
346:16	152:7	<b>Twitter</b> 27:3	360:18	281:22
<b>trouble</b>	154:2,7,17	38:15 65:2	<b>Twitter's</b>	290:5
98:24	154:19	65:8 127:5	282:24	291:21
<b>true</b> 17:25	216:7	146:13,13	289:20	296:20
95:11	219:9	159:18,19	292:5	303:23
211:3	229:1	159:25	<b>Twitter-...</b>	306:8,16
281:1	241:9	162:25	238:11,15	325:12
330:19,22	256:18	163:5	<b>two</b> 21:2,2	331:2,2
331:23	261:22	173:14	21:11,17	332:9
366:21,22	279:19	176:2,6,15	24:9,19	334:3,9
373:13	299:18	199:12,21	29:21	345:14
374:5	300:23	199:23	30:18	356:24
377:9,13	305:1	200:4,9	35:17 37:6	360:23
<b>truly</b> 368:23	306:11	205:17,19	38:23	372:17,18
<b>trust</b> 289:10	314:12	206:1,16	39:18 44:5	<b>two-fifths</b>
289:12,14	315:20	207:25,25	51:16,18	119:10
<b>trusted</b>	323:3,22	208:8	52:8 54:8	<b>two-fold</b>
108:10,14	329:5	209:1,16	59:19,20	265:24
108:18	342:17	210:2	60:10,12	<b>tying</b> 90:11
<b>truth</b> 9:4	346:11	211:16	67:25 75:9	<b>type</b> 27:16
221:18	347:22	212:1,10	86:11 90:3	40:10
319:21	349:14	221:16	90:14	44:12 74:7
344:15	364:2	223:2	101:17	119:25
<b>truths</b>	<b>Tuesday</b>	224:6,7,16	113:24,25	240:16
345:11	226:6	226:9,12	117:7	<b>types</b> 21:3
<b>try</b> 13:1	373:6	226:14,17	119:16,21	21:17
25:1 27:21	<b>turn</b> 139:5	226:22	119:22	243:21
46:3 47:5	<b>turning</b>	227:3	125:11	316:7
47:5 57:10	20:23 24:9	229:16,19	170:3,5	331:19,24
62:20 83:6	37:14	231:4,12	171:3,7,8	<b>typewriting</b>
220:8,19	42:20	233:23	181:3	374:8
229:9	78:19	239:6,6,9	184:25	<b>typical</b>
261:9	177:8	241:5	185:20	177:7,14
314:15	267:4	243:9	188:19	178:8
315:3,8,12	354:4	246:24	191:16	187:11
315:15,25	<b>tweet</b> 224:18	281:8,13	193:18,19	<b>typically</b>
317:10	231:5	281:16,18	193:21	42:11
319:3	289:23	281:23,23	207:22	
332:1	290:2,5,8	282:4	214:20	

U

**LEXITAS LEGAL**

**BRIAN J. SCULLY 1/12/2023**

<b>U</b> 4:1 6:1 7:1 8:1 9:1	13:15,17 16:14 44:15 47:6 48:14 56:23 59:13 79:24 93:7 94:5 143:17 151:2,25 152:19 153:7 154:3,16 219:9 223:13,16 241:12 249:3 256:18 277:13 297:21 304:3 305:20 312:2 314:14 315:1,20 316:9 323:3,7,22 324:7 327:11 343:6 345:9 355:24 358:3,19 358:22 368:23	134:10 143:13 147:17 148:2,17 148:24 154:6 169:6,11 170:17 179:22 182:20 261:10 265:23 266:13 267:18 270:11 279:6 308:12,17 311:8 312:8 325:19 327:17 333:20 336:23 337:16 343:19 365:4	342:1 <b>universe</b> 290:6,7,8 291:8 315:17 359:2 <b>University</b> 46:23,25 46:25 47:1 48:3,18 72:19 360:8 <b>unofficial</b> 281:18 349:22 <b>unoffici...</b> 281:8 <b>unpack</b> 102:11 <b>unrelated</b> 356:17 <b>unsure</b> 90:4 <b>unusual</b> 225:9 <b>upcoming</b> 257:19 299:1 <b>update</b> 129:4 270:13,17 282:6 283:11 <b>updates</b> 128:23 234:23 <b>updating</b> 283:12 <b>upfront</b> 37:20 <b>use</b> 20:13,20 39:22 94:1 94:3 109:20 126:22 138:9 145:22 210:20 231:13 254:18 320:21	<b>useful</b> 140:15 156:7 261:12 314:15 358:8 <b>usefully</b> 144:7 <b>uses</b> 217:16 <b>USG</b> 179:1 216:17 233:13 243:18 245:15 255:21 260:5 262:8 272:10 273:15 274:24 275:7,7,12 275:19,22 287:20 <b>usual</b> 289:1 <b>usually</b> 30:6 233:12 324:1
<b>uh-huh</b> 13:2 <b>uhn-uhn</b> 13:3 <b>Ukraine</b> 322:3 324:6 325:4,7 326:15 <b>ultimate</b> 347:19 <b>umbrella</b> 148:18 <b>unable</b> 92:15 <b>unambiguous</b> 289:24 <b>unauthor...</b> 254:19 <b>unavailable</b> 270:4 <b>unclassi...</b> 25:20 26:9 36:7 235:3 257:4 258:18 <b>unclear</b> 370:21 371:15 <b>undermine</b> 27:21 254:11 283:15 343:10 356:13 <b>undermines</b> 354:24 355:10,19 <b>undermining</b> 27:13 354:21 <b>underneath</b> 28:10 148:19 330:9 <b>underpin...</b> 223:7 <b>understand</b>	<b>understa...</b> 17:15 56:19 59:17 61:19,25 67:22 68:3 68:9,20 73:4 78:13 89:8 107:23 108:1 121:11 122:17 123:23	<b>understood</b> 149:8 158:19 240:7 <b>undertake</b> 240:8 303:12 <b>unfortun...</b> 14:14 237:5 <b>unified</b> 9:9 325:6,14 326:2,6,16 328:13,24 329:1,7 <b>United</b> 1:1 10:9,25 41:12 45:19 90:17 91:5 94:22 95:5 95:12,16 275:7	<b>update</b> 129:4 270:13,17 282:6 283:11 <b>updates</b> 128:23 234:23 <b>updating</b> 283:12 <b>upfront</b> 37:20 <b>use</b> 20:13,20 39:22 94:1 94:3 109:20 126:22 138:9 145:22 210:20 231:13 254:18 320:21	<b>v</b> <b>v</b> 1:8 375:8 376:3 <b>V-i-r-a-...</b> 139:1 <b>vaccine</b> 323:10 <b>vaccines</b> 5:13 144:3 322:1,10 <b>vague</b> 53:1 77:10,11 77:14 87:16 93:2 93:23 130:19 341:6 344:25 <b>validate</b> 224:3 <b>variance</b>

**BRIAN J. SCULLY 1/12/2023**

153:25	347:12	<b>waived</b> 373:7	164:9	261:14
<b>varies</b> 44:21	349:3	<b>wake</b> 335:25	178:2	327:4,21
<b>various</b> 66:3	369:7	<b>walk</b> 18:3	183:12	327:21
298:8	<b>viewed</b> 71:4	<b>walked</b> 54:11	216:2	334:21
351:2	<b>Vijaya</b>	71:1	218:7	341:15
<b>vast</b> 180:21	360:14	<b>Walter</b>	240:6	370:9,13
<b>vehicle</b>	<b>violates</b>	157:18,24	253:23	<b>watch</b> 264:14
61:16	261:6	<b>want</b> 14:20	285:1	279:16
149:14	<b>violations</b>	14:25	287:3,11	<b>watching</b>
<b>vendors</b>	153:5	15:14 27:4	287:25	179:4
264:9	177:4	34:19 42:5	294:9	<b>way</b> 41:11
267:12,13	<b>violence</b>	45:5 56:2	298:24	62:21
<b>venues</b>	340:17	58:3 61:21	343:4	67:18
357:15	366:11,15	63:11 69:5	356:18	81:18
<b>verbal</b> 13:1	<b>VIPs</b> 80:20	77:15 87:7	<b>wanting</b>	84:25 85:8
<b>verifica...</b>	<b>Virality</b>	91:22 92:9	351:23	101:15
288:2	5:11 134:6	93:6 96:3	<b>wants</b> 13:18	108:2
<b>verifying</b>	134:9,15	97:2	315:1	119:25
98:7	135:8,21	113:22	<b>warned</b> 207:1	125:3
<b>Verizon</b>	136:10,18	117:22	<b>warning</b>	133:19
233:24	137:3,17	127:13	207:7	148:23
<b>versus</b> 10:7	138:18,24	133:24	<b>warnings</b>	164:11,20
<b>video</b> 4:20	138:25	149:11	206:22	196:16
10:4 82:24	139:8	154:15	<b>warrant</b>	216:22
145:24	141:14	207:3	207:2	239:22
146:1	144:2	216:6	<b>Warren</b> 43:18	260:18
223:6	<b>visible</b>	221:8	257:15	261:22
224:7	105:9	227:20,23	<b>Washington</b>	273:23
<b>videogra...</b>	<b>voluntary</b>	243:12	2:4 3:21	274:13
10:2,16	318:9,9	249:2	46:23 48:3	280:3
11:8,11	<b>volunteer</b>	252:20	48:19	281:3
34:24 35:2	89:21	253:5	72:20	286:22
83:9,12	<b>vote</b> 8:19	283:11	304:15	300:1,4
183:5,8	302:5,15	300:25	360:9	324:10
209:8,11	<b>votes</b> 217:12	308:21	375:6	327:11
276:6,9	286:14	318:12	<b>wasn't</b> 62:17	337:21
319:10,13	<b>voting</b> 96:11	358:21	63:8 67:12	347:19
362:22,25	96:19	367:18	75:20 76:6	<b>ways</b> 108:4
363:4	<b>voting-r...</b>	372:25	87:8 106:7	119:8,16
372:10	147:3	<b>wanted</b> 30:19	128:6	119:17,22
<b>videos</b> 224:1		30:22	139:12	120:4
<b>Videotaped</b>	<b>W</b>	62:18,25	151:24	159:23
1:14	<b>W</b> 3:9	63:9 65:14	170:5	254:11
<b>view</b> 58:22	<b>wait</b> 14:24	68:15 72:6	175:4	279:3
146:1	<b>waiting</b>	86:19	199:1	283:24
239:8	174:9	121:2	201:7	340:12,20
261:4	212:16	152:6,11	203:5,6	340:24
329:10	252:11	152:12	227:8	342:6
338:22	302:7	163:8,25	238:23	<b>we'll</b> 14:16

**LEXITAS LEGAL**

**BRIAN J. SCULLY 1/12/2023**

34:19 45:6	240:20	170:10,14	213:8	135:24
108:25	243:10	185:15	231:23,25	136:4
207:25	271:11	197:11,15	255:17	137:6
277:14	276:16	197:19	258:7	143:21
279:15	277:5	207:11,13	262:3	149:3
298:7	282:20	210:15	276:19	152:4,6
317:22	289:21	303:10	302:11	159:3
372:23	292:13	<b>weren't</b> 59:2	306:23	169:12,13
<b>we're</b> 28:24	294:10	65:1 152:9	318:22,25	169:22
31:1,17,17	322:18	211:15	341:7	172:1,3,7
34:25 35:3	355:21	239:15	372:9	181:14,17
41:7 44:13	<b>Web</b> 8:7,11	334:13	374:13	182:13,17
45:13	<b>website</b>	<b>Western</b> 1:2	375:15	184:5
125:10	43:13	10:10	376:2,25	185:16
139:13	123:24	<b>WHEREOF</b>	<b>witness's</b>	186:10,13
168:3	138:3	374:13	23:6 97:21	186:23
170:20	365:14,22	<b>White</b> 140:4	345:7	187:5,13
173:5	365:23	140:18	<b>wondering</b>	188:1,4,11
175:23	366:22	<b>whoa</b> 242:22	288:22	196:20
179:3,13	<b>weed</b> 281:9	242:23,23	<b>word</b> 82:9	197:12,15
180:13	281:16	242:23	93:8,11	197:21
183:6	<b>week</b> 86:11	<b>wide</b> 321:9	168:5	229:8
204:7	208:22	<b>Wiki</b> 39:2	341:10	239:14
206:24	283:14	233:25	370:6	240:15
208:21	337:24	<b>Wilson</b>	<b>words</b> 65:2	241:21
209:9	<b>weekend</b>	157:19	68:2 69:6	279:14
224:2	174:16	217:4	69:20	296:7
229:3	<b>weekends</b>	227:18	123:11	304:3,16
235:1	173:25	<b>withdraw</b>	149:4	305:7,11
242:18,19	174:4,6	153:6	160:6	314:13
252:11	<b>weekly</b> 31:23	<b>withdrawal</b>	170:4	315:8
283:12	234:6,11	322:1	180:11	323:16
294:10	234:12,21	324:20	257:16	324:21
302:7	245:24	<b>witness</b>	287:11	325:12
307:14	332:13	10:22 11:2	317:11	343:3,4,8
323:3,22	<b>weeks</b> 19:18	11:9,10	<b>work</b> 16:24	356:6,6
338:16	127:1	14:21,22	17:1 25:9	362:17
343:13	295:15	34:17 35:5	43:3,9,18	364:19,24
346:11	334:3,9	83:3 91:2	43:19,20	368:15,22
348:8	<b>weird</b> 130:7	125:8,11	46:5 47:4	370:18
355:22	269:11	150:21,25	47:15	<b>worked</b> 38:19
356:4,7,8	<b>welcome</b>	152:23	49:14	51:7,19,22
358:20	287:22	153:20	52:13	64:10 66:8
363:1	<b>went</b> 51:14	156:2,10	54:23 89:5	89:3
<b>we've</b> 31:10	58:10 78:8	183:12,14	102:20	104:12
43:3 46:22	85:5,16	190:23	112:18	112:18
69:11	89:5 117:4	191:1	130:22	149:12
181:2	135:3	194:24	131:1,3,9	152:11
192:9	164:25	196:8	131:12	154:20

**LEXITAS LEGAL**

**BRIAN J. SCULLY 1/12/2023**

168:22	171:20	303:2	60:3 62:9	141:5
169:3,7	182:3	329:8	62:10 63:6	143:1
170:15	315:24	<b>wrong</b> 61:20	63:22 65:5	144:12
183:20	316:9	284:9	66:6 67:2	145:9
187:4	323:8	<b>wrongdoing</b>	67:3,24	146:8,18
196:5,9	358:22	153:2	68:1 69:11	147:12
197:8	<b>world</b> 344:14	<b>wrote</b> 209:19	70:1,13	148:13
239:16	<b>worried</b>	211:8	71:24 72:5	149:19
240:24	356:12	229:11	72:14,15	150:1,6,7
266:4	<b>wouldn't</b>	287:23	73:1,4,14	150:8
316:1,4,5	17:23	288:25	74:15	151:10
369:4	41:25	289:25	77:11	152:25
<b>worker</b>	52:18	292:20	78:23 79:1	153:24
217:10	55:14,15	295:13	79:2,19	154:9
218:24	75:15 76:1	312:6,24	80:8 84:7	156:10
219:1,11	80:11	313:3	84:8 86:5	157:13,20
<b>workers</b>	107:6	314:17	86:7,24	158:25
235:20	162:2	316:16	88:3,4	159:21
339:11	169:2	318:2	91:12 92:8	160:12,15
<b>working</b> 31:1	174:18	<b>Wyman</b> 28:6	92:19 93:5	161:14
44:14	177:16	304:14,18	93:17	162:18,23
49:15 51:9	193:14	305:2,4	94:16 96:2	164:15,24
51:16	194:6	353:18	96:12,21	166:3
62:20,25	198:7,7	360:22	96:22 97:2	168:8
142:24	220:1		97:23	169:14
168:24	230:23	<b>X</b>	98:13	174:17
169:4,5,9	235:16	<b>x</b> 1:4,12 5:6	101:12	175:9
169:24,25	236:22	6:1 7:1	102:8	176:25
172:10	237:8	8:1 9:1	103:15	178:2,17
181:22,24	243:19	<b>XII</b> 87:23	104:1	180:9,18
186:15,24	252:1		105:4	183:19
187:6	267:23	<b>Y</b>	106:14	188:3
190:9	296:22,23	<b>yeah</b> 14:22	108:3	189:19
195:23	334:14	15:21	110:24	190:1,25
196:18	339:2	17:25	111:10	192:7
200:2	341:15	18:18 20:3	115:11,21	194:18
226:22	343:21	20:22 23:8	116:5,10	195:16
227:3	347:18	23:15	118:9,18	198:7
233:8	362:18	30:16 31:7	123:21	199:3,24
263:14	368:1	31:9,14,17	124:15	200:5,15
294:10	<b>woven</b> 60:3	33:16,22	125:5,9	200:17
296:22	<b>writing</b>	34:17,18	126:14	201:6,11
297:25	124:12	38:2 42:13	130:14,20	202:17,21
331:5	298:23	42:18	131:17	203:5,19
355:22	<b>written</b> 43:8	45:11	136:25	204:14
356:8	43:9 124:1	47:25 48:9	137:15	208:13,19
<b>works</b> 16:14	188:22	48:21	138:13	209:6
46:4 62:5	190:10	49:22	139:2,25	212:5,12
72:21	299:5	50:19 54:9	140:11	212:19,21

**BRIAN J. SCULLY 1/12/2023**

217:14	287:16	351:17	244:15	<b>z</b>
218:6	288:13,25	354:7,11	245:5	<b>Z-a-h-e-e-r</b>
219:8,14	289:6,25	356:23	249:9	167:7
222:3,18	290:17	359:24	251:5,10	<b>Zaheer</b> 43:14
222:24	291:4,23	360:6,13	253:12	166:19
226:10	292:7	361:21	268:3	167:3
227:14	293:10,11	364:9	269:12,22	171:13,14
228:4,12	294:18,25	369:11,24	272:3,12	179:19
228:22	295:7,13	371:8	283:18	181:11
229:1,2,3	297:6,15	<b>year</b> 19:22	286:9	184:14
229:11,21	298:13	47:23 89:2	287:7,23	185:3,12
231:12,18	299:17	195:23	288:19	191:25
231:20,24	301:13	260:4	289:7	192:12
232:13,20	302:6,9	282:7	293:2	196:25
237:5	304:25	<b>years</b> 12:1	294:12	197:7
239:2,12	305:22	31:13,18	295:16	198:19
239:23	306:1,12	101:5	300:3,3,7	199:6
241:3	308:20	261:20	300:14	276:20
242:1,10	309:11	321:8	304:17	<b>zero</b> 280:12
242:11,22	310:8,14	<b>yep</b> 12:23	312:1,17	<b>zoom</b> 10:13
242:23	310:18,19	48:8 72:9	313:12	14:11,18
244:24	311:21	99:3	316:16	90:23
249:17,19	312:6,24	105:15,19	320:6	<b>o</b>
249:21	313:17	109:5,9	330:12	<b>01/28/2022</b>
250:9,11	314:5,17	110:6,10	331:22	8:20
250:14	315:5,24	111:24	338:14,20	<b>02/11/2022</b>
252:9,14	317:5	119:19	347:2	9:20
252:22,24	319:24	125:16	348:1,10	<b>02/17/2022</b>
253:2,6,9	320:22	126:9	352:25	9:18
253:12	321:11	177:6	355:15	<b>04/14/2022</b>
256:6,22	323:13	191:23	357:4	7:8
258:7	325:1	195:13	361:2	<b>06/18/2020</b>
260:8,25	328:18	196:16	366:7	9:17
262:12,15	329:6,8,17	199:8	368:17,25	<b>06/22/2022</b>
262:16	329:25	200:8	369:25	9:13
264:1	332:21	201:19,21	370:16	<b>08/10/2022</b>
265:7,23	333:9	202:6	<b>Yoel</b> 7:4	9:11
266:10,20	334:8,12	204:10	238:1,2	<b>08/12/2022</b>
269:9,11	334:23	206:23	244:2	8:19
270:2	336:3	210:5,9,23	245:20	<b>09/16/2020</b>
275:9	339:15,20	211:7	289:2,5	7:10
276:4	341:7	222:25	<b>YouTube</b>	<b>1</b>
277:21	342:9,22	225:8	127:6	<b>1</b> 1:22 5:9
278:10,18	344:10,20	226:16	146:13	69:7,10
280:24	345:9	229:25	159:20,24	<b>1.4</b> 108:11
281:7,20	346:20	230:3,10	278:6	109:2
281:25	347:25	230:15	280:10,23	<b>1:41</b> 183:9
283:1,23	348:9	231:3	301:15	
284:21	349:5	233:15		

**BRIAN J. SCULLY 1/12/2023**

10 6:13 87:12 99:9 99:15 212:14,15 212:25 214:10 244:9 276:3 319:7 <b>10/18/2022</b> 8:14 <b>10/31/2022</b> 9:7 <b>10:27</b> 83:10 <b>10:40</b> 83:13 <b>100</b> 26:24 61:15 149:12 <b>101</b> 45:6 <b>10298-300</b> 7:19 <b>10389-391</b> 7:21 <b>10390</b> 288:15 <b>10392-394</b> 7:21 <b>10394</b> 285:16 <b>10410-412</b> 7:22 <b>10420-422</b> 6:16 <b>10449-453</b> 6:15 <b>10492-494</b> 6:12 <b>10512</b> 208:3 <b>10512-516</b> 6:11 <b>10523-526</b> 6:11 <b>10538-541</b> 6:10 <b>10539</b> 204:1 <b>10564-565</b> 7:20 <b>10603</b> 173:9 <b>10603-605</b> 6:7 <b>10679-682</b>	6:6 <b>10718</b> 7:19 281:2 <b>10th</b> 173:14 226:7 286:4 328:21 <b>11</b> 5:3 6:20 108:12,25 109:2,4 173:5 212:14 227:9,12 244:8 245:23 281:6 298:22 <b>11/29/2022</b> 7:6 <b>11:00</b> 175:7 175:10 <b>11:20</b> 292:23 <b>11:21</b> 292:24 <b>11:26</b> 291:20 <b>11:33</b> 292:4 <b>1100</b> 3:20 375:6 <b>11th</b> 281:4 <b>12</b> 1:15 6:22 109:11 110:9 162:9 190:13,16 231:15,19 242:12,19 269:5,9 375:12 376:4 <b>12/01/2020</b> 6:20 <b>12/17/2020</b> 7:5 <b>12:00</b> 175:7 175:10 <b>12:11</b> 226:18 <b>12:34</b> 183:6 <b>12:52</b> 173:19 175:24 <b>12076-079</b>	7:15 <b>12223</b> 297:7 <b>12223-22...</b> 7:23 <b>12th</b> 10:3 302:22 <b>13</b> 7:4 9:22 243:22,25 <b>13599</b> 7:16 <b>13603</b> 214:8 214:10 <b>13603-609</b> 6:15 <b>13661-66...</b> 6:7 <b>13696-701</b> 7:16 <b>13729-734</b> 6:8 <b>138</b> 5:11 <b>138046</b> 1:21 <b>13th</b> 291:18 <b>14</b> 7:6 206:7 206:17 249:15,16 249:17,22 <b>143</b> 146:20 <b>14448</b> 2:6 <b>14526-529</b> 7:14 <b>14545</b> 7:13 269:5,8 <b>14545-547</b> 7:15 <b>14552-553</b> 7:14 <b>15</b> 7:8 87:12 99:9,15 206:1 250:22 252:4,5,16 252:17,18 253:1,8 255:15 330:18,21 331:4,8 337:4,8 <b>156</b> 6:4 <b>15741-743</b>	7:14 <b>15743</b> 261:24 <b>15th</b> 272:6 274:18 294:15 <b>16</b> 7:10 252:5,16 252:17,18 252:18,21 253:1,5 271:21 338:25 <b>1608</b> 375:20 <b>17</b> 7:12 224:16 252:5,16 253:1 259:24 269:4 375:3 <b>17th</b> 248:22 249:6 350:9 374:14 <b>18</b> 7:17 173:10,11 277:16,19 <b>18th</b> 345:24 <b>19</b> 8:4 191:3 191:6,7,8 284:20,21 363:6,9 <b>190</b> 6:22 <b>194</b> 9:24 <b>196</b> 125:2,15 <b>19th</b> 284:19 <b>1st</b> 157:2 271:24 <hr/> <b>2</b> <hr/> <b>2</b> 5:11 89:14 138:17,20 368:12 370:1 <b>2:11</b> 209:9 <b>2:13</b> 209:12 <b>20</b> 117:1 175:25 377:15	<b>200</b> 180:20 189:22 190:2 <b>2018</b> 12:6 31:16,25 32:7 57:7 84:14 117:16 234:7 241:7 244:10 245:2 263:16 <b>2019</b> 12:2 31:25 32:7 195:12 <b>202</b> 3:22 4:8 4:14 <b>2020</b> 5:10 16:23 32:2 32:8 33:5 33:23 35:22 47:24 48:12 51:19 54:13,17 55:14 62:13 63:7 63:15,18 63:25 69:22 72:2 75:21 86:4 86:18 96:6 98:25 107:20 118:11 121:2 126:23 127:9,14 129:15,21 130:18,24 132:21 133:14,25 134:4 147:4,16 149:2,6 151:18,19 153:15
--	--	---	---	--

**LEXITAS LEGAL**



**BRIAN J. SCULLY 1/12/2023**

156:19	<b>2021</b> 5:17, 19	303:18, 24	<b>252</b> 7:8, 10	<b>35</b> 122:2, 4, 8
161:21	5:21 64:3	307:4, 11	7:12	222:20
169:24	69:22	308:22	<b>25th</b> 282:3	<b>352</b> 9:12
170:8	70:10	328:2, 21	<b>27</b> 5:21 8:16	<b>359</b> 9:20
172:18	71:16	334:5, 12	216:25	<b>363</b> 8:4
184:17	88:24	350:9	291:16	<b>364</b> 8:7
185:17	89:10	352:21	301:20	<b>365</b> 8:14
186:7	142:24	362:17	302:1, 8	<b>368</b> 5:14
187:23, 24	167:23	364:16, 25	334:19	<b>369</b> 5:18
189:25	195:12, 14	367:2, 6	335:1, 2, 5	<b>376</b> 1:22
195:19	195:19	<b>2023</b> 1:15	<b>277</b> 7:17	<b>38</b> 231:22, 23
196:13	196:13	10:3 32:10	<b>27th</b> 208:21	232:1, 6, 12
202:14	330:13	32:14	<b>28</b> 8:20	232:13
204:22	331:14	374:14	232:3, 12	242:20, 24
207:15	335:15	375:3, 12	232:14	242:25
208:22	337:5	376:4	306:18, 20	<b>39</b> 242:20
213:16, 18	<b>2022</b> 9:23	<b>2024</b> 8:19	<b>29</b> 8:22	<b>3rd</b> 217:8
214:6	15:9 19:13	19:20	309:20, 23	
234:6, 8, 8	20:24	302:5, 15	<b>2nd</b> 213:17	<b>4</b>
234:9, 11	21:20, 25	302:20	214:14	<b>4</b> 141:15, 16
237:15	22:2, 6	<b>20530</b> 3:21		141:16
241:16, 18	24:12	375:6	<b>3</b>	370:2
241:21	28:16, 24	<b>20th</b> 89:16	<b>3</b> 106:18	<b>4:23</b> 157:2
246:3, 8	33:22	<b>21</b> 8:7 336:5	247:19	<b>4:40</b> 319:6
247:8	34:11	364:11, 14	<b>3:00</b> 175:5	<b>4:42</b> 319:11
248:22	35:16 36:3	<b>211</b> 126:11	<b>3:22-cv-</b> . . .	<b>4:53</b> 319:14
249:6	36:13	126:13	1:8 10:9	<b>40</b> 242:21
255:3	37:15 38:8	<b>212</b> 6:13	<b>3:34</b> 276:7	274:14
262:8, 13	38:24 39:9	<b>213</b> 125:5	<b>3:50</b> 276:10	<b>42</b> 294:4, 6
263:11, 17	41:8, 9	<b>214</b> 125:14	319:5	<b>43</b> 297:17, 20
264:1, 13	52:25 53:7	<b>22053</b> 298:19	<b>30</b> 9:4 144:6	<b>45</b> 298:19
264:19	53:19	<b>221</b> 3:9	144:7	299:15
266:12, 15	54:12, 15	<b>222</b> 251:16	319:15, 18	<b>46</b> 9:12
271:24	55:4 56:8	<b>227</b> 6:20	375:20	224:23, 24
272:6	71:16	<b>229</b> 126:12	<b>301</b> 8:16	298:20
274:18	88:25	<b>22nd</b> 285:25	<b>306</b> 8:20	352:13, 16
282:4	260:4	352:21	<b>309</b> 8:22	<b>475</b> 2:3
283:9	262:13	<b>23</b> 8:11	<b>30th</b> 198:19	<b>48</b> 297:14, 15
284:24	265:8, 11	334:25	199:6	297:16
285:20	265:11, 14	335:7, 12	<b>31</b> 9:8 328:4	<b>48th</b> 297:8
286:4	265:18	<b>23rd</b> 19:18	328:7	<b>49</b> 9:15
291:18	266:8, 21	<b>24</b> 5:17 8:14	<b>319</b> 9:4	297:15
322:19	267:4, 21	288:16	<b>32</b> 349:23	345:19, 20
331:14	268:3, 6	293:9	<b>328</b> 9:8	<b>49th</b> 297:9
332:12	269:7	365:10, 13	<b>33</b> 201:17	
334:3	294:15	<b>24/7</b> 174:9	<b>335</b> 8:11	<b>5</b>
345:24	298:22	267:17	<b>345</b> 9:15	<b>5:46</b> 362:23
348:14	302:22	<b>243</b> 7:4	<b>3484</b> 2:4	<b>5:53</b> 363:1
362:18	303:3, 5, 13	<b>249</b> 7:6	<b>349</b> 9:18	<b>50</b> 319:6

**LEXITAS LEGAL**

**BRIAN J. SCULLY 1/12/2023**

<b>51</b> 203:14	<b>7484-487</b>	<b>8625-627</b>	173:2
<b>514-3259</b>	7:20	7:21	179:13
3:22	<b>751-8870</b>	<b>8628-630</b>	197:25
<b>52</b> 9:18	3:12	6:19	198:10
203:15	<b>7552-554</b>	<b>8631-632</b>	330:6, 8
349:15, 18	7:20	6:19	332:10
349:19	<b>7564-566</b>	<b>8634</b> 6:18	<b>9:06</b> 1:16
350:2	6:10	<b>8636-639</b>	10:4
<b>53</b> 122:5	<b>7565</b> 204:5	6:18	<b>9:32</b> 34:25
<b>54</b> 225:24, 25	<b>7574-576</b> 6:9	<b>864</b> 225:20	<b>9:34</b> 35:3
<b>55</b> 204:1	<b>7583-587</b> 6:9	<b>8640-643</b>	<b>954</b> 225:21
<b>56</b> 162:16	<b>7598-600</b>	6:19	<b>9603-605</b> 6:9
<b>573</b> 3:12	7:15	<b>8649-650</b>	<b>9676</b> 160:22
<b>58</b> 205:10	<b>7599</b> 271:9	6:18	160:24
<b>59</b> 9:20	271:19	<b>8660-662</b>	<b>9676-680...</b>
204:7	<b>7633-634</b> 6:8	6:17	6:6
206:10, 11	<b>7654-659</b>	<b>8663</b> 222:21	<b>9703</b> 7:19
226:4, 5	7:15	222:23	283:7
359:13, 16	<b>7th</b> 261:25	<b>8663-667</b>	<b>9th</b> 98:25
<b>5th</b> 284:24		6:17	282:3
	<b>8</b>	<b>8668-669</b>	
<b>6</b>	<b>8</b> 105:8, 11	6:18	
<b>6</b> 5:14 368:3	297:18	<b>8669</b> 224:21	
368:6	<b>80s</b> 323:25	<b>8679</b> 6:17	
<b>6:04</b> 372:12	323:25	<b>8689</b> 6:17	
373:9	<b>8188-189</b>	<b>8693-694</b>	
<b>6:30</b> 177:3	7:19	6:16	
<b>61</b> 9:22	<b>823848</b> 2:6	<b>8695</b> 6:17	
13:25 14:7	<b>8349</b> 201:20	<b>8696-700</b>	
<b>62</b> 9:24	201:21	6:15	
194:19, 21	<b>8349-352</b> 6:8	<b>870-3578</b> 4:8	
194:22, 25	<b>8356</b> 162:6	<b>8710-711</b>	
198:16	<b>8357</b> 162:14	6:16	
<b>63</b> 208:4	<b>8496-498</b>	<b>8739-741</b>	
<b>64108</b> 375:21	6:11	6:15	
<b>65101</b> 3:11	<b>8519</b> 7:20	<b>8756-758</b>	
<b>69</b> 5:9	284:9	6:12	
<b>6th</b> 223:4	<b>8521-522</b>	<b>8768-769</b>	
	6:16	6:10	
<b>7</b>	<b>8554-557</b>	<b>8769</b> 198:9	
<b>7</b> 5:18	7:23	<b>8778-780</b>	
160:25	<b>8557</b> 294:4	6:12	
292:4	<b>8586-587</b>	<b>899</b> 3:10	
330:4, 5, 5	7:22		
369:17, 21	<b>8595</b> 7:22	<b>9</b>	
369:23	<b>86-3</b> 190:20	<b>9</b> 6:4 156:13	
<b>7:23</b> 226:7, 9	<b>8623-627</b>	156:14	
<b>746-8414</b>	7:22	168:4, 4	
4:14	<b>8625</b> 291:16	170:20	

**LEXITAS LEGAL**

**From:** Misinformation Reports [REDACTED]@cisecurity.org]  
**Sent:** 11/2/2020 4:45:48 PM  
**To:** '[REDACTED]@fb.com']; Misinformation Reports [REDACTED]@cisecurity.org]; Scully, Brian [REDACTED]@cisa.dhs.gov]; CISA Central [REDACTED]@cisa.dhs.gov]; CFITF [REDACTED]@hq.dhs.gov]; tips@2020partnership.atlassian.net  
**Subject:** RE: Case #CIS-MIS000105: votes allegedly being changed in election machines.

**CAUTION:** This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Thank you, [REDACTED]

**From:** [REDACTED]@fb.com>  
**Sent:** Monday, November 2, 2020 4:45 PM  
**To:** Misinformation Reports <[REDACTED]@cisecurity.org>; Brian Scully [REDACTED]@cisa.dhs.gov>; Central CISA [REDACTED]@cisa.dhs.gov>; [REDACTED]@hq.dhs.gov; tips@2020partnership.atlassian.net  
**Subject:** Re: Case #CIS-MIS000105: votes allegedly being changed in election machines.

This has been closed out and the SoS has been informed. Thanks!

**From:** Misinformation Reports [REDACTED]@cisecurity.org>  
**Date:** Monday, November 2, 2020 at 12:07 PM  
**To:** [REDACTED]@fb.com>, Brian Scully [REDACTED]@cisa.dhs.gov>, Central CISA [REDACTED]@cisa.dhs.gov>, [REDACTED]@hq.dhs.gov" [REDACTED]@hq.dhs.gov>, "tips@2020partnership.atlassian.net" <tips@2020partnership.atlassian.net>, Misinformation Reports <[REDACTED]@cisecurity.org>  
**Subject:** Case #CIS-MIS000105: votes allegedly being changed in election machines.

Misinformation report: votes allegedly being changed in election machines.

[REDACTED] – attached and below is a misinformation post on Facebook on the Bullitt County Clerk's Office (KY). Could you please review?

<https://www.facebook.com/bullittcountyclerksoffice/photos/a.237424216303826/3537339692978912/>

Brian and EIP – we are forwarding this report directly to Facebook but still want you to be aware of the issue.

Election Infrastructure Information Sharing and Analysis Center  
 Center for Internet Security  
 Email: [REDACTED]@cisecurity.org  
[www.cisecurity.org](http://www.cisecurity.org)  
 Follow us @CISecurity



**From:** Dearing, Jared (SBE) <[REDACTED]@ky.gov>  
**Sent:** Monday, November 2, 2020 12:37 PM  
**To:** Misinformation Reports <[REDACTED]@cisecurity.org>  
**Subject:** FW: Screenshot 2020-11-02 at 11.41.30 AM

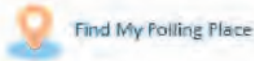
Turning this in for review. -Jared



**Jared Dearing**  
Executive Director

State Board of Elections

a: [REDACTED]  
d: [REDACTED]  
w: www.elect.ky.gov



**From:** [REDACTED]@gmail.com [mailto:[REDACTED]@gmail.com]  
**Sent:** Monday, November 2, 2020 11:45 AM  
**To:** Dearing, Jared (SBE) <[REDACTED]@ky.gov>  
**Subject:** Screenshot 2020-11-02 at 11.41.30 AM

Kevin has asked me to forward this screenshot to you of a comment on our Facebook post this morning.

Thanks  
Ann Oder,DC  
Bullitt County Clerk Office

11:41 ↗



Bullitt County Clerk's Office's Post



Center for official election resources and local updates.

[Get Voting Information](#)



Like



Comment



Share



**Get more Likes, Comments and Shares**

This post is performing better than 85% of other posts on your Page. Boost it to show it to more people.

656 people reached >

**Boost Post**

6

**12 Shares**

**Most Relevant** ▾



**Thomas Botch**

**PROJECTS HAMMER & SCORE CARD - CHANGE VOTES IN THE ACTUAL ELECTION MACHINES - PLEASE INVESTIGATE & SHARE DATA TARGET STEAL 3%**

9m Like Reply



Write a comment...



Sent from my iPhone

.....

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

.....

.....

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

.....

**From:** Scully, Brian [REDACTED]@cisa.dhs.gov]  
**Sent:** 11/2/2020 1:20:01 PM  
**To:** Misinformation Reports [REDACTED]@cisecurity.org; [REDACTED]@fb.com'; [REDACTED]@fb.com]; CISA Central [REDACTED]@cisa.dhs.gov]; CFITF [REDACTED]@hq.dhs.gov]; tips@2020partnership.atlassian.net  
**Subject:** Re: Case #CIS-MIS000105: votes allegedly being changed in election machines.

Sounds good. Thanks!

Brian Scully  
 DHS Countering Foreign Interference Task Force  
 National Risk Management Center

[REDACTED]  
 [REDACTED]@cisa.dhs.gov

**From:** Misinformation Reports [REDACTED]@cisecurity.org>  
**Sent:** Monday, November 2, 2020 1:19:00 PM  
**To:** Scully, Brian [REDACTED]@cisa.dhs.gov>; Misinformation Reports [REDACTED]@cisecurity.org>; [REDACTED]@fb.com'; [REDACTED]@fb.com>; CISA Central [REDACTED]@cisa.dhs.gov>; CFITF [REDACTED]@hq.dhs.gov>; tips@2020partnership.atlassian.net <tips@2020partnership.atlassian.net>  
**Subject:** RE: Case #CIS-MIS000105: votes allegedly being changed in election machines.

**CAUTION:** This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Brian,

For the time being, we will forward Facebook and Instagram related misinformation reports directly to Facebook. We will continue to add you, CISA, and CFITF to the emails for awareness.

Regards,

Election Infrastructure Information Sharing and Analysis Center  
 Center for Internet Security  
 Email: [REDACTED]@cisecurity.org  
[www.cisecurity.org](http://www.cisecurity.org)  
 Follow us @CISecurity

**From:** Scully, Brian [REDACTED]@cisa.dhs.gov>  
**Sent:** Monday, November 2, 2020 1:14 PM  
**To:** Misinformation Reports [REDACTED]@cisecurity.org>; [REDACTED]@fb.com'; [REDACTED]@fb.com>; CISA Central [REDACTED]@cisa.dhs.gov>; [REDACTED]@hq.dhs.gov; tips@2020partnership.atlassian.net  
**Subject:** Re: Case #CIS-MIS000105: votes allegedly being changed in election machines.

Thanks for heads up on sharing with FB. Is that the plan going forward?

Brian Scully  
 DHS Countering Foreign Interference Task Force

National Risk Management Center

[Redacted]

[Redacted]@cisa.dhs.gov

**From:** Misinformation Reports [Redacted]@cisecurity.org>  
**Sent:** Monday, November 2, 2020 1:06:57 PM  
**To:** [Redacted]@fb.com' [Redacted]@fb.com>; Scully, Brian [Redacted]@cisa.dhs.gov>; CISA Central [Redacted]@cisa.dhs.gov>; CFITF [Redacted]@hq.dhs.gov>; tips@2020partnership.atlassian.net <tips@2020partnership.atlassian.net>; Misinformation Reports [Redacted]@cisecurity.org>  
**Subject:** Case #CIS-MIS000105: votes allegedly being changed in election machines.

**CAUTION:** This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Misinformation report: votes allegedly being changed in election machines.

[Redacted] – attached and below is a misinformation post on Facebook on the Bullitt County Clerk’s Office (KY). Could you please review?

<https://www.facebook.com/bullittcountyclerksoffice/photos/a.237424216303826/3537339692978912/>

Brian and EIP – we are forwarding this report directly to Facebook but still want you to be aware of the issue.

Election Infrastructure Information Sharing and Analysis Center  
Center for Internet Security  
Email: [Redacted]@cisecurity.org  
[www.cisecurity.org](http://www.cisecurity.org)  
Follow us @CISecurity

**From:** Dearing, Jared (SBE) [Redacted]@ky.gov>  
**Sent:** Monday, November 2, 2020 12:37 PM  
**To:** Misinformation Reports <[Redacted]@cisecurity.org>  
**Subject:** FW: Screenshot 2020-11-02 at 11.41.30 AM

Turning this in for review. –Jared



**Jared Dearing**  
Executive Director

**State Board of Elections**

a: [Redacted]  
d: [Redacted]  
w: [www.elect.ky.gov](http://www.elect.ky.gov)

Register Online to Vote

Find My Polling Place

Election Calendar

Contact Us



**From:** [REDACTED]@gmail.com [mailto:[REDACTED]@gmail.com]  
**Sent:** Monday, November 2, 2020 11:45 AM  
**To:** Dearing, Jared (SBE) [REDACTED]@ky.gov>  
**Subject:** Screenshot 2020-11-02 at 11.41.30 AM

Kevin has asked me to forward this screenshot to you of a comment on our Facebook post this morning.

Thanks  
Ann Oder\_DC  
Bullitt County Clerk Office

11:41 ↗



Bullitt County Clerk's Office's Post



Center for official election resources and local updates.

[Get Voting Information](#)



Like



Comment



Share



**Get more Likes, Comments and Shares**

This post is performing better than 85% of other posts on your Page. Boost it to show it to more people.

656 people reached >

**Boost Post**

6

**12 Shares**

**Most Relevant** ▾



**Thomas Botch**

**PROJECTS HAMMER & SCORE CARD - CHANGE VOTES IN THE ACTUAL ELECTION MACHINES - PLEASE INVESTIGATE & SHARE DATA TARGET STEAL 3%**

9m Like Reply



Write a comment...



Sent from my iPhone

.....

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

.....

.....

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

.....

**From:** [REDACTED]@fb.com]  
**Sent:** 11/2/2020 6:06:23 PM  
**To:** Misinformation Reports [REDACTED]@cisecurity.org]; Scully, Brian [REDACTED]@cisa.dhs.gov]; CISA Central [REDACTED]@cisa.dhs.gov]; CFITF [REDACTED]@hq.dhs.gov]; tips@2020partnership.atlassian.net  
**Subject:** Re: Case #CIS-MIS000111: Facebook post alleging submitting multiple ballots fraudulently

CAUTION: This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

This has been closed out and the SoS office has been informed. Thanks!

**From:** Misinformation Reports <[REDACTED]@cisecurity.org>  
**Date:** Monday, November 2, 2020 at 4:11 PM  
**To:** [REDACTED]@fb.com>, Brian Scully <[REDACTED]@cisa.dhs.gov>, Central CISA [REDACTED]@cisa.dhs.gov>, [REDACTED]@hq.dhs.gov" [REDACTED]@hq.dhs.gov>, "tips@2020partnership.atlassian.net" <tips@2020partnership.atlassian.net>, Misinformation Reports [REDACTED]@cisecurity.org>  
**Subject:** Case #CIS-MIS000111: Facebook post alleging submitting multiple ballots fraudulently

Misinformation report: Facebook post alleging submitting multiple ballots fraudulently

[REDACTED] – attached and below is a misinformation post on Facebook: <https://www.facebook.com/jamalle.castillo>. Could you please review?

Brian and EIP – we are forwarding this report directly to Facebook but still want you to be aware of the issue.  
 Election Infrastructure Information Sharing and Analysis Center  
 Center for Internet Security  
 Email: [REDACTED]@cisecurity.org  
[www.cisecurity.org](http://www.cisecurity.org)  
 Follow us @CISecurity

**From:** Gookin, Eric [SOS] <[REDACTED]@sos.iowa.gov>  
**Sent:** Monday, November 2, 2020 4:56 PM  
**To:** Misinformation Reports <[REDACTED]@cisecurity.org>  
**Cc:** Doolittle, James <[REDACTED]@hq.dhs.gov>; Judge, Christopher <[REDACTED]@cisa.dhs.gov>; Heidi [SOS] <[REDACTED]@sos.iowa.gov>  
**Subject:** FW: Voter Hotline

FBI #2  
FBI #3

@fbi.gov>; FBI #4 @fbi.gov;  
@fbi.gov>; Burhans,

Please see the below report that we received via email re: FB post.

**From:** Hicok, Wes [SOS] <[REDACTED]@sos.iowa.gov>  
**Sent:** Monday, November 2, 2020 3:36 PM  
**To:** Gookin, Eric [SOS] <[REDACTED]@sos.iowa.gov>; Widen, Molly [SOS] <[REDACTED]@sos.iowa.gov>  
**Subject:** FW: Voter Hotline

We received the below information regarding social media post. The final one is probably of the most concern.

Wesley Hicok

Election Training Specialist  
Office of Secretary of State Paul D. Pate

[REDACTED]

[REDACTED]@sos.iowa.gov

**From:** Jay H [REDACTED]@hotmail.com>  
**Sent:** Monday, November 2, 2020 3:34 PM  
**To:** Hicok, Wes [SOS] [REDACTED]@sos.iowa.gov>  
**Subject:** Re: Voter Hotline



Jamalle's Post



**Lauren Haugh**

Good job- turn Iowa Blue 🇺🇸

2h Like Reply



**Matt Schlabach**

How were the lines?

2h Like Reply



**Jamalle Castillo**

I had absentee ballot(s) that I dropped off.. super fast, but the line for people wanting to vote in person wasn't long at all either

2h Like Reply



Write a reply...



**Ryan Mapus**

Nice!

1h Like Reply



Write a comment...







Jamalle's Post



Jamalle Castillo

3h · 👥

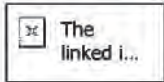
When you are a professional voter fraudelator... you get multiple stickers as a reward for successfully fraudelating!!



Write a comment...







**From:** Hicok, Wes [SOS] [REDACTED]@sos.iowa.gov>  
**Sent:** Monday, November 2, 2020 3:01:16 PM  
**To:** [REDACTED]@hotmail.com <[REDACTED]@hotmail.com>  
**Subject:** RE: VoterHotline

Hello John,

Thank you for contacting the Secretary of State's Office. Secretary Pate asked that I respond to your message.

If you can please forward to me the screen shots you have, we are usually successful in being able to follow up to verify if there is truly malfeasance, or if a person is making an unhelpful claim to discourage others about the process.

Thanks for your time.

Wesley Hicok  
Election Training Specialist  
Office of Secretary of State Paul D. Pate  
[REDACTED]  
[REDACTED]@sos.iowa.gov

-----Original Message-----

**From:** [REDACTED]@sos.iowa.gov <[REDACTED]@sos.iowa.gov>  
**Sent:** Monday, November 2, 2020 2:48 PM  
**To:** Hicok, Wes [SOS] [REDACTED]@sos.iowa.gov>  
**Subject:** VoterHotline

NAME: John [REDACTED]  
PHONE: [REDACTED]  
ADDRESS: [REDACTED]  
CITY: [REDACTED]  
STATE: IA  
ZIP: [REDACTED]  
EMAIL: [REDACTED]@hotmail.com  
COUNTY: [REDACTED]

DATE: 11/1/2020

LOCATION:

DESCRIPTION:

a Facebook post bragging about committing fraud. I have screen shots of the conversation.

CAUTION: This email originated from OUTSIDE of the SOS organization. Do not click on links or open attachments unless you are expecting the email and know that the content is safe. If you believe this to be a malicious or phishing email, please send this email as an attachment to [helpdesk@sos.iowa.gov](mailto:helpdesk@sos.iowa.gov)

CAUTION: This email originated from OUTSIDE of the SOS organization. Do not click on links or open attachments unless you are expecting the email and know that the content is safe. If you believe this to be a malicious or phishing email, please send this email as an attachment to [helpdesk@sos.iowa.gov](mailto:helpdesk@sos.iowa.gov)

.....

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

.....

**From:** [REDACTED] (CELA) [REDACTED]@microsoft.com]  
**Sent:** 11/2/2020 9:36:42 AM  
**To:** Scully, Brian [REDACTED]@cisa.dhs.gov]; [REDACTED] (CELA) [REDACTED]@microsoft.com]; Defending Democracy - Protect 2020 [REDACTED]@microsoft.com]  
**CC:** CFITF [REDACTED]@hq.dhs.gov]  
**Subject:** RE: Case #CIS-MIS000101: phishing emails

**CAUTION:** This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Thanks, Brian!

We passed these to our threat intel folks over the weekend, and we really appreciate the heads up.

[REDACTED]  
 Director, Strategic Projects, Defending Democracy Program  
 Microsoft Digital Diplomacy / Customer Security & Trust  
 [REDACTED]@microsoft.com

C: [REDACTED]

---

**From:** Scully, Brian [REDACTED]@cisa.dhs.gov>  
**Sent:** Saturday, October 31, 2020 5:58 PM  
**To:** [REDACTED] (CELA) [REDACTED]@microsoft.com>; Defending Democracy - Protect 2020 [REDACTED]@microsoft.com>  
**Cc:** CFITF [REDACTED]@hq.dhs.gov>  
**Subject:** [EXTERNAL] Fwd: Case #CIS-MIS000101: phishing emails

Hi [REDACTED].

Please see attached and below reporting of phishing emails from NC.

Regards,

Brian

Brian Scully  
 DHS Countering Foreign Interference Task Force  
 National Risk Management Center  
 [REDACTED]  
 [REDACTED]@cisa.dhs.gov

The Cybersecurity and Infrastructure Security Agency (CISA) of the U.S. Department of Homeland Security (DHS) is not the originator of this information. CISA is forwarding this information, unedited, from its originating source – this

information has not been originated or generated by CISA. This information may also be shared with law enforcement or intelligence agencies.

CISA affirms that it neither has nor seeks the ability to remove or edit what information is made available on social media platforms. CISA makes no recommendations about how the information it is sharing should be handled or used by social media companies. Additionally, CISA will not take any action, favorable or unfavorable, toward social media companies based on decisions about how or whether to use this information.

In the event that CISA follows up to request further information, such a request is not a requirement or demand. Responding to this request is voluntary and CISA will not take any action, favorable or unfavorable, based on decisions about whether or not to respond to this follow-up request for information.

---

**From:** Misinformation Reports <[REDACTED]@cisecurity.org>  
**Sent:** Saturday, October 31, 2020 5:38 PM  
**To:** Scully, Brian; CISA Central; CFITF; Misinformation Reports; [tips@2020partnership.atlassian.net](mailto:tips@2020partnership.atlassian.net)  
**Subject:** Case #CIS-MIS000101: phishing emails

**CAUTION:** This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Brian - Attached are examples of phishing emails received by voters in North Carolina.

EIP – sharing this report in case you are already tracking this issue being shared on social media platforms

---

**From:** Gannon, Patrick <[REDACTED]@ncsbe.gov>  
**Sent:** Saturday, October 31, 2020 5:28 PM  
**To:** Misinformation Reports <[REDACTED]@cisecurity.org>  
**Cc:** Amy Cohen <[REDACTED]@nased.org>  
**Subject:** Phishing/misinformation emails to N.C. voters

Please see the attached emails. Apparently, NC voters are receiving the messages contained within...

Pat

# Patrick Gannon

*Public Information Director*

O: [REDACTED]  
M: [REDACTED]



.....

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

.....

**From:** [REDACTED]@fb.com]  
**Sent:** 11/3/2020 7:07:19 PM  
**To:** Misinformation Reports [REDACTED]@cisecurity.org]; Scully, Brian [REDACTED]@cisa.dhs.gov]; CISA Central [REDACTED]@cisa.dhs.gov]; CFITF [REDACTED]@hq.dhs.gov]; tips@2020partnership.atlassian.net  
**Subject:** Re: Case #CIS-MIS000142: Voter in MI alleges submitting 300 ballots

**CAUTION:** This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Thank you for including me, I'm moving this through our processes now. I'll update you when I have more information.

Best,

Tracy

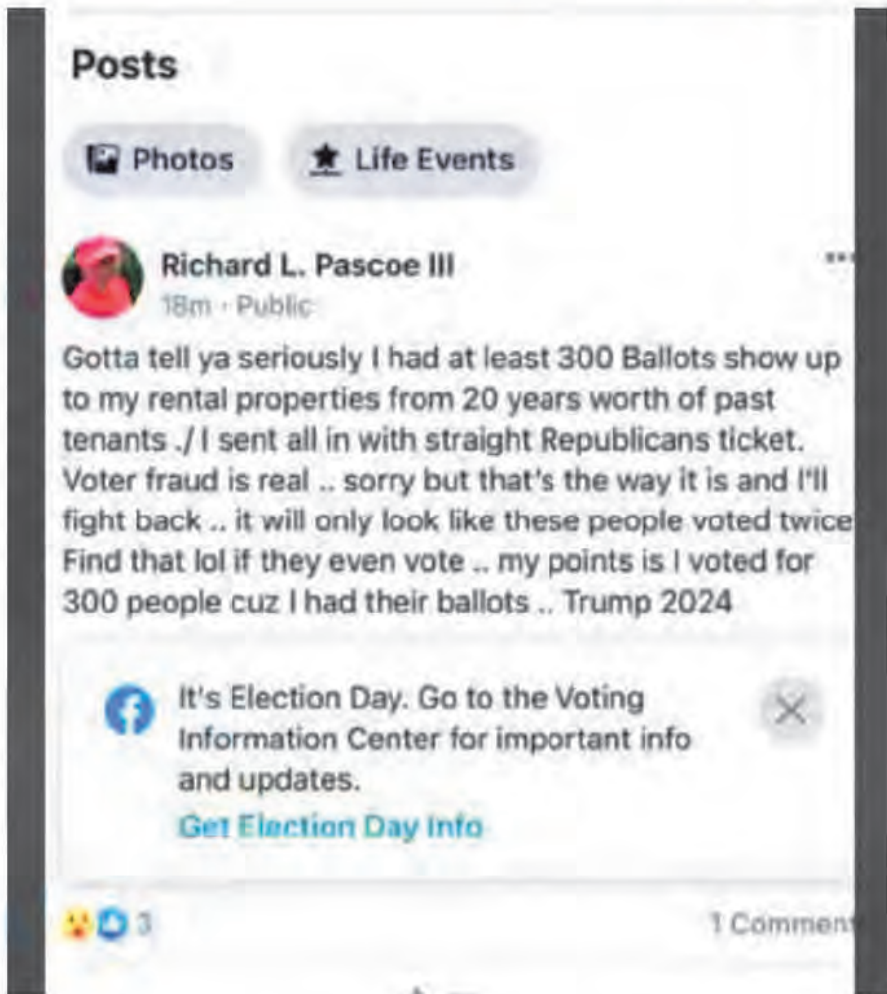
---

**From:** Misinformation Reports [REDACTED]@cisecurity.org>  
**Sent:** Tuesday, November 3, 2020 5:52 PM  
**To:** Brian Scully <[REDACTED]@cisa.dhs.gov>; Central CISA [REDACTED]@cisa.dhs.gov> [REDACTED]@hq.dhs.gov <[REDACTED]@hq.dhs.gov>; tips@2020partnership.atlassian.net <tips@2020partnership.atlassian.net>; Misinformation Reports [REDACTED]@cisecurity.org>  
**Cc:** [REDACTED]@fb.com>  
**Subject:** Case #CIS-MIS000142: Voter in MI alleges submitting 300 ballots

Brian and EIP, we have included Facebook in this report.

Misinformation report: citizen alleges on Facebook that he submitted 300 ballots

<https://www.facebook.com/profile.php?id=1576601744>



From: MS-ISAC SOC  
 Sent: Tuesday, November 3, 2020 6:39 PM  
 To: Misinformation Reports [redacted]@cisecurity.org>  
 Cc: MS-ISAC SOC [redacted]@msisac.org>  
 Subject: FW: Michigan Voter Misinformation//Facebook

Please see below. Thanks.



**Dylan Ginsburg**  
 Security Operations Center Analyst II  
 Multi-State Information Sharing and Analysis Center (MS-ISAC)  
 Election Infrastructure Information Sharing and Analysis Center (EI-ISAC)

[redacted]

24x7 Security Operations Center  
 [redacted]@cisecurity.org - [redacted]



**From:** Brown, Ashiya (MDOS) [REDACTED]@michigan.gov>  
**Sent:** Tuesday, November 3, 2020 6:35 PM  
**To:** MS-ISAC SOC [REDACTED]@msisac.org>  
**Subject:** RE: Michigan Voter Misinformation//Facebook

Yes, please.

Ashiya Brown, MBA  
 Michigan Bureau of Elections  
 [REDACTED]@Michigan.gov  
 Office: [REDACTED]  
 Cell: [REDACTED]

**From:** MS-ISAC SOC [REDACTED]@msisac.org>  
**Sent:** Tuesday, November 3, 2020 6:32 PM  
**To:** Brown, Ashiya (MDOS) [REDACTED]@michigan.gov>; MS-ISAC SOC [REDACTED]@msisac.org>  
**Subject:** RE: Michigan Voter Misinformation//Facebook

**CAUTION: This is an External email. Please send suspicious emails to [abuse@michigan.gov](mailto:abuse@michigan.gov)**

Ashiya,  
 Do we have your permission to share this with our federal partners by forwarding to our misinformation mailbox? Please see below.

*Reports of Elections Infrastructure Misinformation ("Misinformation") submitted to the EI-ISAC via [misinformation@cisecurity.org](mailto:misinformation@cisecurity.org) will be shared with the following organizations: (1) the applicable social media platform provider in order to address the Misinformation identified in the report; (2) the Cybersecurity & Infrastructure Security Agency and the Election Integrity Partnership, for analysis of the Misinformation, in conjunction with other relevant information, to identify potential threats to election security; (3) with the National Association for Secretaries of State and National Association of State Elections Directors for situational awareness. The Misinformation may also be shared with other federal agencies, as appropriate, for situational awareness or in the context of a law enforcement investigation.*





**Dylan Ginsburg**

Security Operations Center Analyst II

Multi-State Information Sharing and Analysis Center (MS-ISAC)

Election Infrastructure Information Sharing and Analysis Center (EI-ISAC)

24x7 Security Operations Center

[REDACTED]@cisecurity.org - [REDACTED]



---

**From:** Brown, Ashiya (MDOS) <[REDACTED]@michigan.gov>**Sent:** Tuesday, November 3, 2020 6:27 PM**To:** MS-ISAC SOC [REDACTED]@msisac.org>**Subject:** Michigan Voter Misinformation//Facebook

<https://www.facebook.com/profile.php?id=1576601744>

Hello,

The link below is a Michigan voter who is spreading misinformation being Facebook saying he voted for 300 people. We have had local law enforcement contact him and he has pulled the post. Hours late (about an hour ago) he started posting it again. Is this something you all can assist with getting Facebook to pull down? We have received a number of complaints about this post per hour.

<https://www.facebook.com/profile.php?id=1576601744>

Thank you!

Ashiya Brown, MBA  
Michigan Bureau of Elections

[REDACTED]@Michigan.gov

Office: [REDACTED]

Cell: [REDACTED]

.....  
This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

.....

.....

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

-----

**From:** Scully, Brian [REDACTED]@cisa.dhs.gov]  
**Sent:** 11/3/2020 4:41:40 PM  
**To:** [REDACTED]@fb.com]  
**CC:** Masterson, Matthew [REDACTED]@cisa.dhs.gov]; [REDACTED]@fb.com]  
**Subject:** Re: EIP-664 Poll worker in Erie PA says announces on Instagram they will throw away Pro-Trump votes

Glad to help. Thanks [REDACTED].

Brian

Brian Scully  
 DHS Countering Foreign Interference Task Force  
 National Risk Management Center  
 [REDACTED]  
 [REDACTED]@cisa.dhs.gov

**From:** [REDACTED]@fb.com>  
**Sent:** Tuesday, November 3, 2020 4:30:26 PM  
**To:** Scully, Brian [REDACTED]@cisa.dhs.gov>  
**Cc:** Masterson, Matthew [REDACTED]@cisa.dhs.gov>; Sandra Luff [REDACTED]@fb.com>  
**Subject:** Re: EIP-664 Poll worker in Erie PA says announces on Instagram they will throw away Pro-Trump votes

**CAUTION:** This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Your speed and helpfulness here is extremely helpful, thank you so much!!!

**From:** Scully, Brian [REDACTED]@cisa.dhs.gov>  
**Sent:** Tuesday, November 3, 2020 4:25:16 PM  
**To:** [REDACTED]@fb.com>  
**Cc:** Masterson, Matthew [REDACTED]@cisa.dhs.gov>; Sandra Luff [REDACTED]@fb.com>  
**Subject:** Re: EIP-664 Poll worker in Erie PA says announces on Instagram they will throw away Pro-Trump votes

Not sure I understand the distinction you're trying to make, but both components of the narrative are false — the person is not a poll worker and no ballots were destroyed. I suppose that makes the entire thing a hoax.

Brian Scully  
 DHS Countering Foreign Interference Task Force  
 National Risk Management Center  
 [REDACTED]  
 [REDACTED]@cisa.dhs.gov

**From:** [REDACTED]@fb.com>  
**Sent:** Tuesday, November 3, 2020 4:22:48 PM  
**To:** Scully, Brian [REDACTED]@cisa.dhs.gov>  
**Cc:** Masterson, Matthew [REDACTED]@cisa.dhs.gov>; [REDACTED]@fb.com>  
**Subject:** Re: EIP-664 Poll worker in Erie PA says announces on Instagram they will throw away Pro-Trump votes

**CAUTION:** This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

P.S. For additional clarity, also trying to confirm here if this entire matter is a hoax versus just the claim a poll worker was destroying ballots.

---

**From:** [REDACTED]@fb.com>  
**Sent:** Tuesday, November 3, 2020, 4:18 PM  
**To:** Scully, Brian  
**Cc:** Masterson, Matthew; [REDACTED]  
**Subject:** Re: EIP-664 Poll worker in Erie PA says announces on Instagram they will throw away Pro-Trump votes

Hello again, wanted to follow up on a few points just to be crystal clear -- could you please confirm that (a) the worker in question is not a pollworker; or (b) that he did not, in fact, destroy ballots (or at least that there is no evidence that he destroyed ballots).

Would appreciate this clarity tremendously, thank you so much.

---

**From:** [REDACTED]@fb.com>  
**Sent:** Tuesday, November 3, 2020 3:57:18 PM  
**To:** Scully, Brian [REDACTED]@cisa.dhs.gov>  
**Cc:** Masterson, Matthew <[REDACTED]@cisa.dhs.gov>; [REDACTED]@fb.com>  
**Subject:** Re: EIP-664 Poll worker in Erie PA says announces on Instagram they will throw away Pro-Trump votes

Appreciate the swift response!!

---

**From:** Scully, Brian [REDACTED]@cisa.dhs.gov>  
**Sent:** Tuesday, November 3, 2020 3:52:45 PM  
**To:** [REDACTED]@fb.com>  
**Cc:** Masterson, Matthew [REDACTED]@cisa.dhs.gov>  
**Subject:** Fwd: EIP-664 Poll worker in Erie PA says announces on Instagram they will throw away Pro-Trump votes

Statement from PA. Confirms person was not poll worker.

Brian

Brian Scully  
DHS Countering Foreign Interference Task Force  
National Risk Management Center  
[REDACTED]  
[REDACTED]@cisa.dhs.gov

---

**From:** CFITF [REDACTED]@hq.dhs.gov>  
**Sent:** Tuesday, November 3, 2020 3:43:52 PM  
**To:** CFITF All [REDACTED]@hq.dhs.gov>  
**Subject:** FW: EIP-664 Poll worker in Erie PA says announces on Instagram they will throw away Pro-Trump votes

---

**From:** ██████████@cisecurity.org  
**Sent:** Tuesday, November 3, 2020 8:43:42 PM (UTC+00:00) Monrovia, Reykjavik  
**To:** CFITF  
**Subject:** EIP-664 Poll worker in Erie PA says announces on Instagram they will throw away Pro-Trump votes

**CAUTION:** This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

---

Reply above this line.

██████████@cisecurity.org commented:

The county has issued an official statement on the matter:



[View request](#) · [Turn off this request's notifications](#)

This is shared with Facebook, EI-ISAC, Twitter, and Mike Caulfield.

Powered by Jira Service Desk

**Sent:** 11/3/2020 11:14:52 AM  
**To:** [REDACTED]@google.com]  
**CC:** CFITF [REDACTED]@hq.dhs.gov]  
**Subject:** FW: Case#CIS-MIS000101:phishing emails  
**Attachments:** OnTime Notification: Incident Number [#NCSBE-64073] Changed; OnTime Notification: Incident Number [#NCSBE-64071] Changed

Hey Richard,

Wanted to share the attached and below reporting of phishing emails from North Carolina.

Regards,  
 Brian

**From:** Misinformation Reports <[REDACTED]@cisecurity.org>  
**Sent:** Saturday, October 31, 2020 5:38 PM  
**To:** Scully, Brian <[REDACTED]@cisa.dhs.gov>; CISA Central <[REDACTED]@cisa.dhs.gov>; CFITF <[REDACTED]@hq.dhs.gov>; Misinformation Reports <[REDACTED]@cisecurity.org>; tips@2020partnership.atlassian.net  
**Subject:** Case #CIS-MIS000101: phishing emails

**CAUTION:** This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Brian - Attached are examples of phishing emails received by voters in North Carolina.

EIP – sharing this report in case you are already tracking this issue being shared on social media platforms

**From:** Gannon, Patrick <[REDACTED]@ncsbe.gov>  
**Sent:** Saturday, October 31, 2020 5:28 PM  
**To:** Misinformation Reports <[REDACTED]@cisecurity.org>  
**Cc:** Amy Cohen <[REDACTED]@nased.org>  
**Subject:** Phishing/misinformation emails to N.C. voters

Please see the attached emails. Apparently, NC voters are receiving the messages contained within...

Pat

**Patrick Gannon**

*Public Information Director*

O: [REDACTED]

M: [REDACTED]



.....  
This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

.....

From: [REDACTED]@twitter.com]  
 Sent: 11/4/2020 8:22:49 AM  
 To: Scully, Brian [REDACTED]@cisa.dhs.gov]  
 CC: [REDACTED]@twitter.com]; [REDACTED]@twitter.com]; mailto:[REDACTED]@twitter.com [REDACTED]@twitter.com]; CFITF [REDACTED]@hq.dhs.gov] [REDACTED]@cisecurity.org  
 Subject: Re: FW: Case #CIS-MIS000152: Misinformation tweet that tabulation machines use ink (Green Bay, WI)

**CAUTION:** This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Thank Brian. We will escalate.

On Wed, Nov 4, 2020 at 8:21 AM Scully, Brian [REDACTED]@cisa.dhs.gov> wrote:  
 Please see below report from NASED.

Regards,  
 Brian

*The Cybersecurity and Infrastructure Security Agency (CISA) of the U.S. Department of Homeland Security (DHS) is not the originator of this information. CISA is forwarding this information, unedited, from its originating source – this information has not been originated or generated by CISA. This information may also be shared with law enforcement or intelligence agencies.*

*CISA affirms that it neither has nor seeks the ability to remove or edit what information is made available on social media platforms. CISA makes no recommendations about how the information it is sharing should be handled or used by social media companies. Additionally, CISA will not take any action, favorable or unfavorable, toward social media companies based on decisions about how or whether to use this information.*

*In the event that CISA follows up to request further information, such a request is not a requirement or demand. Responding to this request is voluntary and CISA will not take any action, favorable or unfavorable, based on decisions about whether or not to respond to this follow-up request for information.*

From: Misinformation Reports [REDACTED]@cisecurity.org>  
 Sent: Wednesday, November 4, 2020 7:59 AM  
 To: Scully, Brian [REDACTED]@cisa.dhs.gov>; CISA Central [REDACTED]@cisa.dhs.gov>; CFITF [REDACTED]@hq.dhs.gov>; [tips@2020partnership.atlassian.net](mailto:tips@2020partnership.atlassian.net); Misinformation Reports [REDACTED]@cisecurity.org>  
 Subject: Case #CIS-MIS000152: Misinformation tweet that tabulation machines use ink (Green Bay, WI)

**CAUTION:** This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.


Misinformation report: tweet alleges tabulation machine ran out of ink which caused delay in counting absentee ballots---there is no ink involved in tabulation machine (Green Bay, WI)



 **Tweet****Reid J. Epstein**  @reidepstein · 2h

Green Bay's absentee ballot results are being delayed because one of the vote-counting machines ran out of ink and an elections official had to return to City Hall to get more.

 427 3K 4K

**From:** Amy Cohen @nased.org>  
**Sent:** Wednesday, November 4, 2020 7:45 AM  
**To:** Misinformation Reports <[misinformation@cisecurity.org](mailto:misinformation@cisecurity.org)>  
**Subject:** Tweet

<https://twitter.com/reidepstein/status/1323926165590052864?s=21>

This is false. There is no ink involved in the machines used in tabulation of the ballots, a fact confirmed by the state: [https://twitter.com/wi\\_elections/status/1323931755473240066?s=21](https://twitter.com/wi_elections/status/1323931755473240066?s=21)

Amy Cohen  
Executive Director  
National Association of State Election Directors (NASED)

.....  
This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

.....

**From:** Misinformation Reports [REDACTED]@cisecurity.org]  
**Sent:** 11/3/2020 3:53:03 PM  
**To:** Scully, Brian [REDACTED]@cisa.dhs.gov]; CISA Centra [REDACTED]@cisa.dhs.gov]; CFITF [REDACTED]@hq.dhs.gov]; tips@2020partnership.atlassian.net; Misinformation Reports [REDACTED]@cisecurity.org]  
**CC:** [REDACTED]@fb.com; [REDACTED]@fb.com]  
**Subject:** Case #CIS-MIS000133: Misinformation Facebook post regarding number of votes/voters in CO

**CAUTION:** This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Brian and EIP, we have included Facebook in this report.

Misinformation report: Facebook post regarding number of votes/voters in Colorado

**From:** Josh Craven <[REDACTED]@SOS.STATE.CO.US>  
**Sent:** Tuesday, November 3, 2020 3:44 PM  
**To:** Misinformation Reports <[REDACTED]@cisecurity.org>  
**Cc:** Trevor Timmons <[REDACTED]@sos.state.co.us>; Craig Buesing [REDACTED]@SOS.STATE.CO.US>; Aaron Hayman <[REDACTED]@SOS.STATE.CO.US>; Nathan Blumenthal [REDACTED]@SOS.STATE.CO.US>; Judd Choate [REDACTED]@sos.state.co.us>; Hilary Rudy <[REDACTED]@SOS.STATE.CO.US>  
**Subject:** Potential Foreign Mis/Dis Information on the Election Process – Facebook Post

Partners,

As part of the Colorado Department of State's (CDOS) efforts to counter foreign mis/dis information on the election process, we have been made aware of the following inaccurate information. We know this information is false because we've had 2,893,395 vote out of a possible 3,783,589 registered voters. This is not a call to action, but merely providing for you information.

<https://www.facebook.com/dpatric/posts/10223827649629519>



**Disclaimer:** Colorado Department of State is not the originator of the above information and is forwarding it, unedited, from its original source. The Department does not seek the ability to remove or edit what information is made available on social media platforms. The Department makes no recommendations about how the information it is sharing should be handled or used by recipients of this email. The Department may also share this information with local, state, and federal government agencies.

Thanks,



Josh Craven  
 Election Security Specialist | Department of State  
 [Redacted]  
 [Redacted] [@SOS.STATE.CO.US](mailto:[Redacted]@SOS.STATE.CO.US)

.....  
 This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

.....

**From:** [REDACTED]@fb.com]  
**Sent:** 11/3/2020 7:14:18 PM  
**To:** Misinformation Reports [REDACTED]@cisecurity.org]; Scully, Brian [REDACTED]@cisa.dhs.gov]; CISA Central [REDACTED]@cisa.dhs.gov]; CFITF [REDACTED]@hq.dhs.gov]; tips@2020partnership.atlassian.net  
**Subject:** Re: Case #CIS-MIS000137: Facebook post alleging election fraud

**CAUTION:** This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Confirming that this has been closed out and the SoS has been notified. Thanks!

**From:** Misinformation Reports [REDACTED]@cisecurity.org>  
**Date:** Tuesday, November 3, 2020 at 4:03 PM  
**To:** Brian Scully [REDACTED]@cisa.dhs.gov>, Central CISA [REDACTED]@cisa.dhs.gov>, [REDACTED]@hq.dhs.gov" <[REDACTED]@hq.dhs.gov>, "tips@2020partnership.atlassian.net" <tips@2020partnership.atlassian.net>,  
 Misinformation Reports [REDACTED]@cisecurity.org>  
**Cc:** [REDACTED]@fb.com>  
**Subject:** Case #CIS-MIS000137: Facebook post alleging election fraud

Brian and EIP, we have included Facebook in this report.

Misinformation report: Facebook post alleging election fraud

<https://www.facebook.com/photo/?fbid=10213886606959482&set=a.1076542573951>

**From:** Dearing, Jared (SBE) [REDACTED]@ky.gov>  
**Sent:** Tuesday, November 3, 2020 4:56 PM  
**To:** Misinformation Reports [REDACTED]@cisecurity.org>  
**Subject:** Miss information

Someone sent this to me said that Christy Alley the actress tweeted this and that it's now going viral this is Miss information.

Get [Outlook for iOS](#)

.....

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

.....

**From:** [REDACTED]@twitter.com]  
**Sent:** 11/6/2020 12:15:08 PM  
**To:** Scully, Brian [REDACTED]@cisa.dhs.gov]  
**CC:** CFITF [REDACTED]@hq.dhs.gov]  
**Subject:** Re: FW: Are these real?

**CAUTION:** This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Thank you so much! We have applied a label to the Tweet.

Thanks,  
[REDACTED]

On Fri, Nov 6, 2020 at 11:58 AM Scully, Brian <[REDACTED]@cisa.dhs.gov> wrote:

Hey Stacia,

Just came across this debunk of the video on Twitter --  
<https://twitter.com/JaneLvty/status/1324756117415776257?s=20>.

Brian

---

**From:** [REDACTED]@twitter.com>  
**Sent:** Friday, November 6, 2020 9:53 AM  
**To:** Scully, Brian [REDACTED]@cisa.dhs.gov>  
**Cc:** CFITF [REDACTED]@hq.dhs.gov>  
**Subject:** Re: FW: Are these real?

**CAUTION:** This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Thanks, Brian. We recognize the PA Secretary of State might be busy at this moment. I am happy to escalate now without waiting for additional information.

Thanks,  
[REDACTED]

On Fri, Nov 6, 2020 at 9:51 AM Scully, Brian <[REDACTED]@cisa.dhs.gov> wrote:

Hey [REDACTED]

There are two reports in this email chain. One of Facebook posts with videos the State believes are false. That was the basis of the FYI for another group of folks. The specific report we are sharing with you all is the most recent link to a Twitter post. The FYI does not apply to the Twitter portion of the chain (unless

I'm misreading things, which in my current state is possible). We are not allowed to edit the reporting emails, so it creates some challenges for us when we're forwarding such reports.

On the video's authenticity, PA states in the very first email that they believe the video's are false. We are reaching out to partners to validate. Not sure we'll be able to get a validation, but can certainly pass along anything we get back.

Not sure this is helpful, so happy to chat if you'd like.

Brian

---

**From:** CFITF [REDACTED]@hq.dhs.gov>  
**Sent:** Friday, November 6, 2020 9:41 AM  
**To:** CFITF All <[REDACTED]@hq.dhs.gov>  
**Subject:** FW: FW: Are these real?

---

**From:** [REDACTED]  
**Sent:** Friday, November 6, 2020 2:40:46 PM (UTC+00:00) Monrovia, Reykjavik  
**To:** CFITF; Scully, Brian  
**Cc:** [REDACTED]@twitter.com; [REDACTED]@twitter.com; [REDACTED]@twitter.com  
**Subject:** Re: FW: Are these real?

**CAUTION:** This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Also, have PA state officials provided additional information to you on the authenticity of video or circumstances underpinning it? It seems as if the correspondence flagging this issue to you said "FYI only at this point" and there isn't additional information from the state official.

Thank you,  
[REDACTED]

On Fri, Nov 6, 2020 at 9:35 AM [REDACTED] <[REDACTED]@twitter.com> wrote:

Thank you CFITF. We only see one URL linking to a video, but no attached screenshots as were referenced in the email. Please let us know if there are additional materials you would like us to review?

Thanks,  
[REDACTED]

On Fri, Nov 6, 2020 at 9:34 AM CFITF <[REDACTED]@hq.dhs.gov> wrote:

**Good morning Twitter – Please see the reporting below.**

---

**From:** Masterson, Matthew [REDACTED]@cisa.dhs.gov>  
**Sent:** Friday, November 6, 2020 9:19 AM  
**To:** Scully, Brian [REDACTED]@cisa.dhs.gov>; Dragseth, John [REDACTED]@cisa.dhs.gov>  
**Subject:** FW: Are these real?

See more below from PA. have we heard anything?

Matthew V. Masterson  
Senior Cybersecurity Advisor  
Department of Homeland Security  
Cybersecurity & Infrastructure Security Agency (CISA)  
[REDACTED]  
[REDACTED]@hq.dhs.gov

---

**From:** Myers, Jessica [REDACTED]@pa.gov>  
**Sent:** Friday, November 6, 2020 9:16 AM  
**To:** Masterson, Matthew [REDACTED]@cisa.dhs.gov>  
**Subject:** Fwd: Are these real?

**CAUTION:** This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Here's a little more. Any word on your side? We just got a request from a reporter. We know the one on our page was taken down, but it appears there are more floating out there.

Jessica C. Myers  
Director of Policy  
PA Department of State  
[REDACTED]

---

**From:** Yabut, Danilo <[REDACTED]@pa.gov>  
**Sent:** Friday, November 6, 2020 6:29 AM  
**To:** Myers, Jessica; Parker, Scott  
**Cc:** Moser, Michael; Swanger, Zane  
**Subject:** RE: Are these real?

I think I found a version of the video: <https://twitter.com/StateofusAll/status/1324556436135882753>

Dan

---

**From:** Yabut, Danilo  
**Sent:** Friday, November 6, 2020 3:35 AM  
**To:** Myers, Jessica <[REDACTED]@pa.gov>; Parker, Scott <[REDACTED]@pa.gov>  
**Cc:** Moser, Michael <[REDACTED]@pa.gov>; Swanger, Zane <[REDACTED]@pa.gov>  
**Subject:** RE: Are these real?

Thank you for the notice. If you got screenshots or links can you send those?

Dan

---

**From:** Myers, Jessica <[REDACTED]@pa.gov>  
**Sent:** Friday, November 6, 2020 12:01 AM  
**To:** Yabut, Danilo <[REDACTED]@pa.gov>; Parker, Scott <[REDACTED]@pa.gov>  
**Cc:** Moser, Michael <[REDACTED]@pa.gov>; Swanger, Zane <[REDACTED]@pa.gov>  
**Subject:** Fwd: Are these real?

FYI only at this point

Jessica C. Myers  
Director of Policy  
PA Department of State  
[REDACTED]

---

**From:** Myers, Jessica <[REDACTED]@pa.gov>  
**Sent:** Thursday, November 5, 2020 11:36 PM  
**To:** Matt Masterson (DHS)  
**Subject:** Re: Are these real?

The only guess I have is, if this is real, they took live feed from "remaking" damaged ballots. I just have no idea where this might have come from..

Jessica C. Myers  
Director of Policy  
PA Department of State



[REDACTED]

---

**From:** Myers, Jessica <[REDACTED]@pa.gov>  
**Sent:** Thursday, November 5, 2020 11:22:52 PM  
**To:** Matt Masterson (DHS) <[REDACTED]@hq.dhs.gov>  
**Subject:** Are these real?

Matt,

Sorry to message late, but was going through the dos page and comments (old habits from EAC die hard) and came across these posts. Sorry to screenshot, but if you go to our page you should be able to see the comments on the post and go to the pages.

Are these making their way around the internet? Because there is no polling place I know of that has overhead cameras. Just don't want another "burning ballots" fake thing spreading.

Apologies for sending to you all first, but I didn't want to call an all hands meeting here when some of our folks are getting their first few real hours rest since Monday.

Thanks,

Jess

From: CFITF [REDACTED]@hq.dhs.gov]  
 Sent: 11/6/2020 3:45:24 PM  
 To: [REDACTED]@twitter.com]; Josiah, Chad [REDACTED]@cisa.dhs.gov]; Scully, Brian [REDACTED]@cisa.dhs.gov]  
 CC: [REDACTED]@twitter.com; [REDACTED]@twitter.com  
 Subject: Re: FW: Case#CIS-MIS000184: alleged tabulation fraud in Delaware County, PA

Thank you for the update, Stacia.

From: [REDACTED]@twitter.com>  
 Sent: Friday, November 6, 2020 12:43:27 PM  
 To: Josiah, Chad [REDACTED]@cisa.dhs.gov>; Scully, Brian <[REDACTED]@cisa.dhs.gov>  
 Cc: [REDACTED]@twitter.com [REDACTED]@twitter.com>; [REDACTED]@twitter.com <[REDACTED]@twitter.com>; CFITF <cfitf@hq.dhs.gov>  
 Subject: Re: FW: Case #CIS-MIS000184: alleged tabulation fraud in Delaware County, PA

**CAUTION:** This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Hi Chad, all four Tweets have been labeled.

Thank you!

On Fri, Nov 6, 2020 at 2:26 PM [REDACTED] <[REDACTED]@twitter.com> wrote:  
 Thanks, Chad. We will review.

On Fri, Nov 6, 2020 at 2:15 PM Josiah, Chad <[REDACTED]@cisa.dhs.gov> wrote:  
 Twitter team,

Please see below reporting from official.

Regards,

Chad Josiah

*The Cybersecurity and Infrastructure Security Agency (CISA) of the U.S. Department of Homeland Security (DHS) is not the originator of this information. CISA is forwarding this information, unedited, from its originating source – this information has not been originated or generated by CISA. This information may also be shared with law enforcement or intelligence agencies.*

*CISA affirms that it neither has nor seeks the ability to remove or edit what information is made available on social media platforms. CISA makes no recommendations about how the information it is sharing should be handled or used by social media companies. Additionally, CISA will not take any action, favorable or unfavorable, toward social media companies based on decisions about how or whether to use this information.*

*In the event that CISA follows up to request further information, such a request is not a requirement or demand. Responding to this request is voluntary and CISA will not take any action, favorable or unfavorable, based on decisions about whether or not to respond to this follow-up request for information.*

**From:** CFITF <[REDACTED]@hq.dhs.gov>  
**Sent:** Friday, November 6, 2020 2:10 PM  
**To:** CFITF All <[REDACTED]@hq.dhs.gov>  
**Subject:** FW: Case #CIS-MIS000184: alleged tabulation fraud in Delaware County, PA

---

**From:** Misinformation Reports  
**Sent:** Friday, November 6, 2020 7:10:09 PM (UTC+00:00) Monrovia, Reykjavik  
**To:** Scully, Brian; CISA Central; CFITF; [tips@2020partnership.atlassian.net](mailto:tips@2020partnership.atlassian.net); Misinformation Reports  
**Subject:** Case #CIS-MIS000184: alleged tabulation fraud in Delaware County, PA

**CAUTION:** This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Misinformation report: tweets alleging tabulation fraud in Delaware County, PA

---

**From:** Sam Derheimer <[REDACTED]@hartic.com>  
**Sent:** Friday, November 6, 2020 1:59 PM  
**To:** Misinformation Reports <[REDACTED]@cisecurity.org>  
**Cc:** Amy Cohen <[REDACTED]@nased.org>  
**Subject:** Misinformation from Delaware County, PA

Good morning,

I think you guys are likely already aware of this, but there is misinformation spreading widely about the counting/tabulation process in Delaware County, PA. The county is a Hart customer, and they contacted us about this, so I am sharing it. I've already seen some posts containing the video removed by Twitter, so it appears that these posts are already being flagged.

A video is widely circulating of election workers in Delaware County duplicating ballots that could not be read by scanners. This is a routine election procedure. However, the video was doctored to cut out the observers who were present at the site. It artificially looks like the election worker is filling out blank ballots unsupervised. Most of the posts claim the workers are filling out blank ballots in an apparent attempt to "steal" the election.

1. From the [London Daily News](#).
2. From Drudge Report-knockoff site called [Populist Press](#).

This [Tweet](#) previously also shared the video, with the claim that the election was being “stolen,” but it has already been removed by Twitter.

Here are some other Tweets with the video that are still live:

1. [Andrew Wilkow](#)
2. [Anna Paulina Luna](#)
3. [Josh Kandelstick](#)

Sharing out of an abundance of caution, in case you weren't already aware. Please let me know if you need further information.

**Samuel Derheimer**

Director of Government Affairs

**Hart InterCivic**

██████████ (o) ██████████ (help desk)

██████████ (efax) | <http://www.hartintercivic.com>

This message (including any attachments) is intended only for the use of the individual or entity to which it is addressed and may contain information that is non-public, proprietary, privileged, confidential, and exempt from disclosure under applicable law or may constitute as attorney work product. If you are not the intended recipient, you are hereby notified that any use, dissemination, distribution, or copying of this communication is strictly prohibited. If you have received this communication in error, notify us immediately by telephone and (i) destroy this message if a facsimile or (ii) delete this message immediately if this is an electronic communication. Thank you.

.....

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

**From:** [REDACTED]@fb.com]  
**Sent:** 11/4/2020 12:48:44 PM  
**To:** Misinformation Reports [REDACTED]@cisecurity.org]; Scully, Brian [REDACTED]@cisa.dhs.gov]; CISA Central [REDACTED]@cisa.dhs.gov]; CFITF [REDACTED]@hq.dhs.gov]; tips@2020partnership.atlassian.net  
**Subject:** Re: Case #CIS-MIS000153: alleged election fraud in Graves County, KY

**CAUTION:** This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

This has been closed out and the SoS has been informed. Thanks!

**From:** Misinformation Reports <[REDACTED]@cisecurity.org>  
**Date:** Wednesday, November 4, 2020 at 10:11 AM  
**To:** Brian Scully <[REDACTED]@cisa.dhs.gov>, Central CISA [REDACTED]@cisa.dhs.gov>, [REDACTED]@hq.dhs.gov" <[REDACTED]@hq.dhs.gov>, "tips@2020partnership.atlassian.net" <tips@2020partnership.atlassian.net>, Misinformation Reports <[REDACTED]@cisecurity.org>  
**Cc:** [REDACTED]@fb.com>  
**Subject:** Case #CIS-MIS000153: alleged election fraud in Graves County, KY

Brian and EIP, we have included Facebook in this report.

Misinformation report: Facebook post alleging election fraud in Graves County, KY

<https://www.facebook.com/glenn.hayden.370>

**From:** Dearing, Jared (SBE) <[REDACTED]@ky.gov>  
**Sent:** Wednesday, November 4, 2020 10:42 AM  
**To:** Misinformation Reports <[REDACTED]@cisecurity.org>  
**Subject:** Misinformation

Can you have this taken down. This is Misinformation voters were not given the incorrect ballots.

-Jared

Get [Outlook for iOS](#)

.....  
 This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

.....

**From:** Misinformation Reports [REDACTED]@cisecurity.org]  
**Sent:** 11/5/2020 5:18:37 PM  
**To:** Scully, Brian [REDACTED]@cisa.dhs.gov]; CISA Central [REDACTED]@cisa.dhs.gov]; CFITF [REDACTED]@hq.dhs.gov]; tips@2020partnership.atlassian.net; Misinformation Reports [REDACTED]@cisecurity.org]  
**CC:** [REDACTED]@fb.com; [REDACTED]@fb.com]  
**Subject:** Case #CIS-MIS000177: Facebook post alleging election fraud  
**Attachments:** 177.PNG

**CAUTION:** This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Brian and EIP – we have included Facebook in this report.

Misinformation Report: Facebook post alleging election fraud

**From:** Elections HelpDesk <[REDACTED]@wisconsin.gov>  
**Sent:** Thursday, November 5, 2020 12:53 PM  
**To:** Magney, Reid - ELECTIONS <[REDACTED]@wisconsin.gov>  
**Subject:** FW: FW:

**From:** [REDACTED]@charter.net>  
**Sent:** Thursday, November 05, 2020 12:46 PM  
**To:** Elections HelpDesk <elections@wisconsin.gov>  
**Subject:** FW:

There are some very frightening statements being posted. I believe this is absolutely garbage. Is there a way to debunk this before it spreads farther.

[https://m.facebook.com/story.php?story\\_fbid=10157811093171886&id=569891885&sfnsn=mo](https://m.facebook.com/story.php?story_fbid=10157811093171886&id=569891885&sfnsn=mo)

Sent from my Galaxy

.....  
 This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

.....

**From:** [REDACTED]@fb.com]  
**Sent:** 11/6/2020 12:00:12 PM  
**To:** Misinformation Reports [REDACTED]@cisecurity.org]; Scully, Brian [REDACTED]@cisa.dhs.gov]; CISA Central [REDACTED]@cisa.dhs.gov]; CFITF [REDACTED]@hq.dhs.gov]; tips@2020partnership.atlassian.net  
**Subject:** Re: Case #CIS-MIS000182: Misinformation post that Trump already won AZ

**CAUTION:** This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

We have closed the loop with the partner on this one. Thanks all.

--  
 [REDACTED]  
 U.S. Politics & Government Outreach  
 E: [REDACTED]  


---

**From:** [REDACTED]@fb.com>  
**Date:** Friday, November 6, 2020 at 10:14 AM  
**To:** Misinformation Reports <[REDACTED]@cisecurity.org>, Brian Scully [REDACTED]@cisa.dhs.gov>, Central CISA [REDACTED]@cisa.dhs.gov>, [REDACTED]@hq.dhs.gov" [REDACTED]@hq.dhs.gov>, "tips@2020partnership.atlassian.net" <tips@2020partnership.atlassian.net>  
**Cc:** [REDACTED]@azsos.gov" <[REDACTED]@azsos.gov>  
**Subject:** Re: Case #CIS-MIS000182: Misinformation post that Trump already won AZ

Thanks for sending this over – we're looking into it.

--  
 [REDACTED]  
 U.S. Politics & Government Outreach  
 E: [REDACTED]@fb.com  


---

**From:** Misinformation Reports <[REDACTED]@cisecurity.org>  
**Date:** Friday, November 6, 2020 at 10:09 AM  
**To:** Brian Scully <[REDACTED]@cisa.dhs.gov>, Central CISA <[REDACTED]@cisa.dhs.gov>, [REDACTED]@hq.dhs.gov" [REDACTED]@hq.dhs.gov>, "tips@2020partnership.atlassian.net" <tips@2020partnership.atlassian.net>, Misinformation Reports [REDACTED]@cisecurity.org>  
**Cc:** [REDACTED]@fb.com>  
**Subject:** Case #CIS-MIS000182: Misinformation post that Trump already won AZ

Brian and EIP, I included Facebook in this report.

Misinformation report: (private) Facebook post that Trump already won AZ

---

**From:** Ken Matta [REDACTED]@azsos.gov>  
**Sent:** Friday, November 6, 2020 9:54 AM

To: Misinformation Reports <[REDACTED]@cisecurity.org>  
Subject: Fake statement by Arizona Election Worker about fraud

Hi There.

<https://www.facebook.com/photo.php?fbid=3966754973352465&set=p.3966754973352465&type=3>

This post was on a private FB page, above. I've included a screenshot.

Thank you!



**KATIE HOBBS**  
SECRETARY OF STATE  
State of Arizona

Ken Matta  
Information Security Officer  
Arizona Secretary of State's Office

Email: [REDACTED]@azsos.gov  
Office: [REDACTED]  
Cell: 602-[REDACTED]

*This message and any messages in response to the sender of this message may be subject to a public records request.*

.....  
This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.  
.....



**From:** [REDACTED]@fb.com]  
**Sent:** 11/10/2020 12:17:57 PM  
**To:** Misinformation Reports [REDACTED]@cisecurity.org]; Scully, Brian [REDACTED]@cisa.dhs.gov]; CISA Central [REDACTED]@cisa.dhs.gov]; CFITF [REDACTED]@hq.dhs.gov]; tips@2020partnership.atlassian.net  
**Subject:** Re: Case #CIS-MIS000192:allegations that a deceased person voted in Monona County, Iowa

**CAUTION:** This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

This case has been closed out and the Secretary of State's office has been informed. Thanks!

**From:** Misinformation Reports <[REDACTED]@cisecurity.org>  
**Date:** Monday, November 9, 2020 at 5:29 PM  
**To:** Brian Scully <[REDACTED]@cisa.dhs.gov>, Central CISA <central@cisa.dhs.gov>, [REDACTED]@hq.dhs.gov" <[REDACTED]@hq.dhs.gov>, "tips@2020partnership.atlassian.net" <tips@2020partnership.atlassian.net>, Misinformation Reports [REDACTED]@cisecurity.org>  
**Cc:** [REDACTED]@fb.com>  
**Subject:** Case #CIS-MIS000192: allegations that a deceased person voted in Monona County, Iowa

Brian and EIP, we have included Facebook in this report.

Misinformation report: Facebook post that a deceased person voted in Monona County, Iowa

<https://www.facebook.com/amy.zeitler>

**From:** Gookin, Eric [SOS] <[REDACTED]@sos.iowa.gov>  
**Sent:** Monday, November 9, 2020 6:05 PM  
**To:** Misinformation Reports <[REDACTED]@cisecurity.org>  
**Cc:** Franklin, Jeff [SOS] <[REDACTED]@sos.iowa.gov>; Hall, Kevin [SOS] <[REDACTED]@sos.iowa.gov>  
**Subject:** RE: Facebook post

Slight correction on information from below. The voter's record was cancelled due to his death on 10/05/2009, NOT in 1999.

**From:** Gookin, Eric [SOS]  
**Sent:** Monday, November 9, 2020 5:02 PM  
**To:** Misinformation Reports <[REDACTED]@cisecurity.org>  
**Cc:** Franklin, Jeff [SOS] <[REDACTED]@sos.iowa.gov>; Hall, Kevin [SOS] <[REDACTED]@sos.iowa.gov>  
**Subject:** FW: Facebook post

Good afternoon,

We received this email from a local election official about a FB post saying a deceased person voted. Attached is a screen shot of the post along with a scanned copy of the voter's cancelled VR record.

**From:** Franklin, Jeff [SOS] <[REDACTED]@sos.iowa.gov>  
**Sent:** Monday, November 9, 2020 4:30 PM

To: Gookin, Eric [SOS] <[REDACTED]@sos.iowa.gov>  
 Subject: FW: Facebook post

Are you reporting these or is comms?

From: Peggy Rolph <[REDACTED]@mononacounty.org>  
 Sent: Friday, November 6, 2020 9:10 AM  
 To: cyber [REDACTED]@sos.iowa.gov>  
 Subject: Facebook post

Good Morning,

I reached out to Wes at Secretary of State's office and he informed me to get this information to you. I received a complaint about a Facebook post that implies a deceased person had voted. I have attached the post from Facebook and my record from I Voters to show you that the person is deceased and has been a canceled vote since 8/18/1999. We also do not have a precinct named ON204. My office received a call from this person's mother yesterday and she was upset. I then had another citizen come into my office wanting to know how this was posted on Facebook. We received another phone call this morning from the step father wanting to know how this is happening. I hope that you can assist with this matter.

*Peggy A. Rolph  
 Monona County Auditor &  
 Commissioner of Elections*

[REDACTED]  
 [REDACTED]  
 [REDACTED]  
 Fax [REDACTED]

[REDACTED]@mononacounty.org

*"Believe you can and you're halfway there." - Theodore Roosevelt*

CAUTION: This email originated from OUTSIDE of the SOS organization. Do not click on links or open attachments unless you are expecting the email and know that the content is safe. If you believe this to be a malicious or phishing email, please send this email as an attachment to [helpdesk@sos.iowa.gov](mailto:helpdesk@sos.iowa.gov)

.....  
 This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.  
 .....

**From:** Misinformation Reports [REDACTED]@cisecurity.org]  
**Sent:** 11/11/2020 8:51:20 PM  
**To:** Scully, Brian [REDACTED]@cisa.dhs.gov]; CISA Central [REDACTED]@cisa.dhs.gov]; CFITF [REDACTED]@hq.dhs.gov]; tips@2020partnership.atlassian.net; Misinformation Reports [REDACTED]@cisecurity.org]  
**CC:** [REDACTED]@twitter.com  
**Subject:** Case #CIS-MIS000197: allegations of election fraud in Kentucky  
**Attachments:** 197.PNG

**CAUTION:** This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Brian and EIP, we have included Twitter in this report.

Twitter, please see below the Misinformation Report submitted by the office of the Secretary of State of Kentucky: tweet alleging election fraud in Kentucky

---

**From:** Dearing, Jared (SBE) [REDACTED]@ky.gov>  
**Sent:** Wednesday, November 11, 2020 8:39 PM  
**To:** Misinformation Reports <misinformation@cisecurity.org>  
**Subject:**

<https://twitter.com/kimmyann1111/status/1326584103844544512?s=12>

These facts are not correct and are spreading misinformation.

-Jared

Get [Outlook for iOS](#)

.....  
This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

.....

**From:** Misinformation Reports [REDACTED]@cisecurity.org]  
**Sent:** 11/11/2020 6:07:35 PM  
**To:** [REDACTED]@twitter.com  
**CC:** CISA Central [REDACTED]@cisa.dhs.gov]; CFITF [REDACTED]@hq.dhs.gov]; Scully, Brian [REDACTED]@cisa.dhs.gov];  
**Subject:** Misinformation Reports [REDACTED]@cisecurity.org]  
Fwd: Case #CIS-MIS000196: allegations of election fraud

**CAUTION:** This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Twitter,

Please see below a Misinformation Report submitted by the Kentucky Secretary of State office.

Because today is a holiday, we are forwarding this report directly to you.

Election Infrastructure Information Sharing and Analysis Center

Center for Internet Security

Email: [REDACTED]@cisecurity.org

[www.cisecurity.org](http://www.cisecurity.org)

Begin forwarded message:

**From:** Misinformation Reports [REDACTED]@cisecurity.org>  
**Date:** November 11, 2020 at 4:49:18 PM EST  
**To:** Brian Scully [REDACTED]@cisa.dhs.gov>, CISA Central [REDACTED]@cisa.dhs.gov>, CISA CFITF [REDACTED]@hq.dhs.gov>, EIP <tips@2020partnership.atlassian.net>, Misinformation Reports [REDACTED]@cisecurity.org>  
**Subject:** Case #CIS-MIS000196: allegations of election fraud

Twitter account alleging election fraud: <https://twitter.com/DianeKnudsen7>

---

**From:** Dearing, Jared (SBE) [REDACTED]@ky.gov>  
**Sent:** Wednesday, November 11, 2020 4:28 PM  
**To:** Misinformation Reports [REDACTED]@cisecurity.org>  
**Subject:** Missinformation

This user is pushing miss information about election fraud that does not exist. looking at the entire account it looks like bot trolling activity if not an out right disinformation account.

-Jared

Get [Outlook for iOS](#)

.....



This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

**From:** [REDACTED]@twitter.com]  
**Sent:** 11/11/2020 10:06:41 PM  
**To:** Scully, Brian [REDACTED]@cisa.dhs.gov]  
**CC:** [REDACTED]@twitter.com]; [REDACTED]@twitter.com]; Twitter Government & Politics [REDACTED]@twitter.com]; CFITF [REDACTED]@hq.dhs.gov]; Misinformation Reports [REDACTED]@cisecurity.org]  
**Subject:** Re: FW: CIS-MIS000198 - allegations of election fraud in Kentucky

**CAUTION:** This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Thanks, Brian. We will escalate.

On Wed, Nov 11, 2020 at 9:54 PM Scully, Brian <[REDACTED]@cisa.dhs.gov> wrote:  
 Team Twitter,

Please see the below report from KY.

Regards,

Brian

*The Cybersecurity and Infrastructure Security Agency (CISA) of the U.S. Department of Homeland Security (DHS) is not the originator of this information. CISA is forwarding this information, unedited, from its originating source – this information has not been originated or generated by CISA. This information may also be shared with law enforcement or intelligence agencies.*

*CISA affirms that it neither has nor seeks the ability to remove or edit what information is made available on social media platforms. CISA makes no recommendations about how the information it is sharing should be handled or used by social media companies. Additionally, CISA will not take any action, favorable or unfavorable, toward social media companies based on decisions about how or whether to use this information.*

*In the event that CISA follows up to request further information, such a request is not a requirement or demand. Responding to this request is voluntary and CISA will not take any action, favorable or unfavorable, based on decisions about whether or not to respond to this follow-up request for information.*

**From:** Misinformation Reports [REDACTED]@cisecurity.org>  
**Sent:** Wednesday, November 11, 2020 9:44 PM  
**To:** Scully, Brian <[REDACTED]@cisa.dhs.gov>; CISA Central <[REDACTED]@cisa.dhs.gov>; CFITF <[REDACTED]@hq.dhs.gov>; tips@2020partnership.atlassian.net; Misinformation Reports [REDACTED]@cisecurity.org>  
**Subject:** CIS-MIS000198 - allegations of election fraud in Kentucky

**CAUTION:** This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.



Misinformation report: series of tweets alleging election fraud in Kentucky

**From:** Dearing, Jared (SBE) [REDACTED]@ky.gov>  
**Sent:** Wednesday, November 11, 2020 9:23 PM  
**To:** Misinformation Reports <[REDACTED]@cisecurity.org>  
**Subject:** Misinformation

<https://twitter.com/grassrootsspeak/status/1326593623522152450?s=12>

These facts are incorrect and this user is spreading misinformation.

-Jared

Get [Outlook for iOS](#)

.....

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

.....

**From:** [REDACTED]@twitter.com]  
**Sent:** 11/12/2020 9:27:50 AM  
**To:** Scully, Brian [REDACTED]@cisa.dhs.gov]  
**CC:** CFITF [REDACTED]@hq.dhs.gov]; Misinformation Reports [REDACTED]@cisecurity.org]; [REDACTED]  
[REDACTED]@twitter.com]; [REDACTED]@twitter.com]  
**Subject:** Re: CIS-MIS000199 - allegations of election fraud in Kentucky

**CAUTION:** This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Thanks Brian. We will escalate.

On Thu, Nov 12, 2020 at 9:26 AM Scully, Brian [REDACTED]@cisa.dhs.gov> wrote:

Good morning Twitter,

Please see reporting from KY.

Thanks,

Brian

*The Cybersecurity and Infrastructure Security Agency (CISA) of the U.S. Department of Homeland Security (DHS) is not the originator of this information. CISA is forwarding this information, unedited, from its originating source – this information has not been originated or generated by CISA. This information may also be shared with law enforcement or intelligence agencies.*

*CISA affirms that it neither has nor seeks the ability to remove or edit what information is made available on social media platforms. CISA makes no recommendations about how the information it is sharing should be handled or used by social media companies. Additionally, CISA will not take any action, favorable or unfavorable, toward social media companies based on decisions about how or whether to use this information.*

*In the event that CISA follows up to request further information, such a request is not a requirement or demand. Responding to this request is voluntary and CISA will not take any action, favorable or unfavorable, based on decisions about whether or not to respond to this follow-up request for information.*

Brian Scully  
DHS Countering Foreign Interference Task Force  
National Risk Management Center  
(202) 450-8046  
[brian.scully1@cisa.dhs.gov](mailto:brian.scully1@cisa.dhs.gov)

---

**From:** CFITF <[REDACTED]@hq.dhs.gov>  
**Sent:** Thursday, November 12, 2020 8:51:35 AM

**To:** CFITF All [REDACTED]@hq.dhs.gov>  
**Subject:** FW: CIS-MIS000199 - allegations of election fraud in Kentucky

---

**From:** Misinformation Reports  
**Sent:** Thursday, November 12, 2020 1:51:17 PM (UTC+00:00) Monrovia, Reykjavik  
**To:** Scully, Brian; CISA Central; CFITF; [tips@2020partnership.atlassian.net](mailto:tips@2020partnership.atlassian.net); Misinformation Reports  
**Subject:** CIS-MIS000199 - allegations of election fraud in Kentucky

**CAUTION:** This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Misinformation report: five (5) tweets alleging election fraud in Kentucky.

**From:** Dearing, Jared (SBE) [REDACTED]@ky.gov>  
**Sent:** Wednesday, November 11, 2020 11:27 PM  
**To:** Misinformation Reports [REDACTED]@cisecurity.org>  
**Subject:** Misinformation

This is misinformation and is being spread repeatedly can you please search for similar content that is being put out on your platform.

<https://twitter.com/vammek/status/1326683752357978112?s=12>

<https://twitter.com/lillygrillzit/status/1326649213468332032?s=12>

<https://twitter.com/skywalkeranakn/status/1326706794891243521?s=12>

<https://twitter.com/vammek/status/1326705839760027648?s=12>

<https://twitter.com/vammek/status/1326683637664772098?s=12>

-Jared  
Executive Director  
Kentucky State Board of Elections

Get [Outlook for iOS](#)

.....

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

.....

From: [REDACTED]@twitter.com]  
 Sent: 11/11/2020 12:11:52 AM  
 To: Scully, Brian [REDACTED]@cisa.dhs.gov]  
 CC: [REDACTED]@twitter.com]; [REDACTED]@twitter.com]; Twitter Government & Politics [REDACTED]@twitter.com]; CFITF [REDACTED]@hq.dhs.gov]; Misinformation Reports [REDACTED]@cisecurity.org]  
 Subject: Re: FW: Case #CIS-MIS000195: allegations of election fraud with Dominion voting equipment in WA state

**CAUTION:** This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Thank you. All Tweets have been labeled, with the exception of two from @SeattleSuze. Those two Tweets were not found to violate our policies.

Thank you,  
 [REDACTED]

On Tue, Nov 10, 2020 at 7:25 PM [REDACTED]@twitter.com> wrote:  
 Thanks, Brian. We will escalate.

On Tue, Nov 10, 2020 at 7:23 PM Scully, Brian [REDACTED]@cisa.dhs.gov> wrote:  
 Good evening Twitter,

Please see the below report from Washington.

Thanks,  
 Brian

*The Cybersecurity and Infrastructure Security Agency (CISA) of the U.S. Department of Homeland Security (DHS) is not the originator of this information. CISA is forwarding this information, unedited, from its originating source – this information has not been originated or generated by CISA. This information may also be shared with law enforcement or intelligence agencies.*

*CISA affirms that it neither has nor seeks the ability to remove or edit what information is made available on social media platforms. CISA makes no recommendations about how the information it is sharing should be handled or used by social media companies. Additionally, CISA will not take any action, favorable or unfavorable, toward social media companies based on decisions about how or whether to use this information.*

*In the event that CISA follows up to request further information, such a request is not a requirement or demand. Responding to this request is voluntary and CISA will not take any action, favorable or unfavorable, based on decisions about whether or not to respond to this follow-up request for information.*

**From:** Misinformation Reports <[misinformation@cisecurity.org](mailto:misinformation@cisecurity.org)>  
**Sent:** Tuesday, November 10, 2020 7:17 PM

**To:** Scully, Brian <[REDACTED]@cisa.dhs.gov>; CISA Central <[REDACTED]@cisa.dhs.gov>; CFITF <[REDACTED]@hq.dhs.gov>; [tips@2020partnership.atlassian.net](mailto:tips@2020partnership.atlassian.net); Misinformation Reports <[REDACTED]@cisecurity.org>

**Subject:** Case #CIS-MIS000195: allegations of election fraud with Dominion voting equipment in WA state

**CAUTION:** This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Misinformation report: twelve (12) tweets alleging election fraud with Dominion voting equipment in Washington state.

---

**From:** Jacob, Nick <[REDACTED]@sos.wa.gov>

**Sent:** Tuesday, November 10, 2020 7:03 PM

**To:** Misinformation Reports <[REDACTED]@cisecurity.org>

**Cc:** Lori Augino <[REDACTED]@sos.wa.gov>; Zabel, Kylee <[REDACTED]@sos.wa.gov>; Boyal, Kiran <[REDACTED]@sos.wa.gov>

**Subject:** Misinformation on Twitter

Hello,

I wanted to flag the following tweets that include misinformation and/or false allegations of election fraud. There is no evidence to back any of these claims. There have been no reports or indications of fraudulent activity in Washington state for the 2020 general election.

Franklin County is the only county in Washington state that uses a version of Dominion software and hardware. The system in use has been certified, and we are not aware of any issues.

No counties in Washington state use GEMS.

Additionally, each county conducts post-election audits in the days after the election that are publicly observable, which provides another layer of protection to ensure the results they certify later this month are accurate. At the end of the certification period, each county will publish a reconciliation report that discloses details about all of the ballots issued, received, counted, and rejected during this election.

<https://twitter.com/LuvMyCountry7/status/1326303394147921920>

<https://twitter.com/seattleSuze/status/1326208987348398080>

<https://twitter.com/seattleSuze/status/1326209828717436928>

<https://twitter.com/MatthewMacphe17/status/1326212450585210880>

<https://twitter.com/MatthewMacphe17/status/1326211588089470976>

<https://twitter.com/MatthewMacphe17/status/1326204530543882240>

<https://twitter.com/MatthewMacphe17/status/1326202866567049216>

<https://twitter.com/Katrina64718085/status/1326311025738575872>

<https://twitter.com/Maga2020Rules/status/1326187323566948352>

<https://twitter.com/lazalere/status/1326082445196681216>

<https://twitter.com/TerenaHimpel/status/1326006222034665472>

<https://twitter.com/LolaTwelve/status/1325934941503250433>

My name is Nick Jacob, and I'm an Executive Receptionist for the Washington Office of the Secretary of State. I can be reached via this email or the number listed in my signature block below. My cell phone is monitored after hours if I need to be reached urgently.

I am also copying Washington State Elections Director Lori Augino, Office of the Secretary of State Communications Director Kylee Zabel, and our Web and Social Media Coordinator Kiran Boyal.

Please let me know if you have any questions or need additional information.

Thank you.

-Nick

### **Nick Jacob**

Office of the Secretary of State

Cell: [REDACTED]



Secretary of State

*Tina Wynn*



.....  
This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.  
.....



**CONFIDENTIAL**

**IN THE UNITED STATES DISTRICT COURT  
WESTERN DISTRICT OF LOUISIANA**

**The State of Missouri and the State of  
Louisiana,**

*Plaintiffs,*

v.

**President Joseph R. Biden, Jr., in his  
official capacity as President of the United  
States of America, et. al.,**

*Defendants.*

Civil Action No. 22-cv-1213

**DEFENDANTS’ AMENDED COMBINED OBJECTIONS AND RESPONSES TO  
PLAINTIFFS’ FIRST SET OF EXPEDITED  
PRELIMINARY-INJUNCTION RELATED INTERROGATORIES**

Pursuant to Federal Rules of Civil Procedure 26 and 33 and the Local Rules of the U.S. District Court for the Western District of Louisiana, Defendants, by and through counsel, provide the following combined objections and responses to Plaintiffs’ First Set of Expedited Preliminary-Injunction Related Interrogatories (“Plaintiffs’ First PI Interrogatories” or “Interrogatories”) served on July 18, 2022 on the following Defendants: Dr. Anthony Fauci; Centers for Disease Control and Prevention (“CDC”); Surgeon General Vivek H. Murthy; U.S. Department of Health and Human Services (“HHS”); National Institute of Allergy and Infectious Diseases (“NIAID”); U.S. Department of Homeland Security (“DHS”); Cybersecurity and Infrastructure Security Agency (“CISA”); Jen Easterly, Director of CISA; Nina Jankowicz (former Executive Director of the DHS Disinformation Governance Board); and White House Press Secretary Karine Jean-Pierre (collectively, “Defendants”). Consistent with the agreement of the parties, Defendants have combined the objections and responses to address duplication of certain interrogatories among

**CONFIDENTIAL**



**CONFIDENTIAL**

Defendants but have addressed each interrogatory for each Defendant to which each interrogatory is directed. Defendants have amended these objections and responses in a manner consistent with the Court's September 6, 2022, Order (ECF No. 72).

Defendants' combined objections and responses are based on information known to Defendants at this time and are made without prejudice to additional objections should Defendants subsequently identify additional grounds for objection. The objections have been formulated in contemplation of Federal Rule of Civil Procedure 26(b)(1), which generally permits discovery of matters not privileged that may be relevant to the claims or defenses in a civil action. In presenting their objections, Defendants do not waive any further objection in pretrial motions practice or at trial to the admissibility of evidence on the grounds of relevance, materiality, privilege, competency, or any other appropriate ground.

### **OBJECTIONS TO DEFINITIONS AND INSTRUCTIONS**

1. Defendants object to the definitions of "Content Modulation," and the related term "Misinformation," including to the extent that Plaintiffs' definition of "Content Modulation" covers actions by Social Media Companies *beyond* those taken against content containing Misinformation and against users posting content containing Misinformation (such as actions taken as to any post on "efficacy of COVID-19 restrictions" or on "security of voting by mail"). For purposes of these Responses and Objections, Defendants generally define "Misinformation" in a manner consistent with Plaintiffs' definition of that term: "any form of speech . . . considered to be potentially or actually incorrect, mistaken, false, misleading, lacking proper context, disfavored, having the tendency to deceive or mislead . . . including but not limited to any content or speech considered by any federal official or employee or Social-Media Platform to be 'misinformation,' 'disinformation,' 'malinformation,' 'MDM,' 'misinfo,' 'disinfo,' or

**CONFIDENTIAL**

**CONFIDENTIAL**

‘malinfo.’” *See* Interrogatories, Definition O.

2. Defendants object to the definitions of CDC, CISA, DHS, HHS, NIAID, and White House Communications Team to the extent those definitions include “any . . . agent,” “contractors” and “any subordinate agency or entity” of those agencies on the ground that those definitions are overbroad and may include persons and entities that are not under the supervision or control of any Defendant. In particular, HHS and DHS also object to the extent any Interrogatory seeks a Department-wide response as unduly burdensome and disproportionate to the needs of the case. As the least burdensome sources of information consistent with Rules 26 and 33 that is potentially responsive to the Interrogatories, (i) DHS has identified its Headquarters (HQ), and (ii) HHS has identified the Office of the Surgeon General (OSG), NIAID, and CDC, and the four HHS employees identified in the Court’s September 6, 2022 Order. Further, Defendant also objects to the definition of “White House Communications Team” for the additional reason that such a definition is not proportional to the needs of the case to the extent Plaintiffs seek information beyond the possession of the White House Office of the Press Secretary upon which Plaintiffs served Interrogatories.

3. The individual Defendants Dr. Fauci, Dr. Murthy, Ms. Easterly, and Ms. Jean-Pierre, construe the Complaint and Amended Complaint as seeking relief against them each in their official capacity as head of agencies of various components of agencies or other offices of the Federal Government, including NIAID, HHS, CISA, and the Office of the White House Press Secretary, and, accordingly, each individual Defendant objects or responds to each Interrogatory exclusively through his or her corresponding agency Defendant. Individual Defendant Jankowicz has no successor in office, and the Disinformation Governance Board is paused. Moreover, DHS interprets any relief sought as against Ms. Jankowicz in her official capacity within DHS HQ,

**CONFIDENTIAL**

**CONFIDENTIAL**

and, accordingly, she objects or responds to each Interrogatory exclusively through DHS. Defendants object to any Interrogatory seeking from an individual Defendant a response that can be provided by that individual Defendant's corresponding agency in a manner that is less burdensome to Defendants and proportional to the needs of the case.

4. Defendants object to the definition of "communication" to the extent it is meant to cover anything beyond e-mail exchanges, as overbroad and disproportional to the needs of the case, particularly in light of the expedited nature of the discovery now ongoing

5. Defendants object to the definition of "document" to the extent it includes "documents retained on personal devices and/or in personal e-mail accounts or other personal accounts." Documents found on personal devices or within electronic personal accounts would not be in the custody or control of any Defendant. Defendants further object on the grounds that this definition is an unwarranted invasion of the privacy of non-parties and seeks information protected by the Privacy Act, 5 U.S.C. § 552a, et seq.

6. Defendants object to the definition of "identify" to the extent it calls for disclosure of information covered by any applicable privilege or protection over, among other elements, a person's "email address, and present or last known address and telephone number

7. Defendants object to the use of the undefined term "Meeting" in a manner incompatible with, and calculating to expand the obligations imposed by, the Government in the Sunshine Act, 5 U.S.C. 552b.

8. Defendants object to the definition of "Social-Media Platform" as overbroad, because it includes "any organization that provides a service for public users to disseminate . . . content . . . to other users or the public," along with any "contractors, or any other person . . . acting on behalf of the Social-Media Platform . . . as well [as] subcontractors or entities used to

**CONFIDENTIAL**

**CONFIDENTIAL**

conduct fact-checking or any other activities relating to Content Modulation.” Such a definition is overbroad because the Complaint (and the Amended Complaint) contains no nonconclusory allegation that Defendants communicated with each and every organization that allows users to “disseminate . . . content” to other users, along with any persons or entities affiliated with those organizations. Defendants will construe “Social-Media Platform” to encompass Facebook, Instagram, Twitter, LinkedIn, and YouTube.

9. Defendants object to the definition of “You” an “Your” in each Interrogatory as overbroad, as it includes “any officers, officials, employees, agents, staff members, contractors, and other(s)” acting at the direction, or on behalf, of any Defendant served with any Interrogatory. Such a definition also is not proportional to the needs of the case, especially given the expedited, abbreviated discovery process in which Defendants have only a limited amount of time to respond to Plaintiffs’ Interrogatories. Defendants interpret any Interrogatory relying on this definition as applying solely to the named Defendants upon whom the Interrogatory was served insofar as a response to such Interrogatory by such Defendant is consistent with Rules 26 and 33. In particular, Plaintiffs’ allegations against each individual Defendant concerns actions taken in that individual’s official capacity, and, accordingly, the agency Defendant corresponding to and that employed each individual Defendant is the proper party for objecting and responding to Plaintiffs’ Interrogatories, as explained in Paragraphs 2 and 3 above.

10. Defendant Jean-Pierre objects to the definition of “You” and “Your” as overbroad as it includes “any officers, officials, employees, agents, staff members, contractors, or other(s) acting at the direction of Jennifer Rene Psaki, in her official capacity as Press Secretary, or at the direction of her successor.” Such a definition is not proportional to the needs of the case to the extent it is interpreted to extend beyond the Office of the White House Press Secretary, especially

**CONFIDENTIAL**

**CONFIDENTIAL**

given the expedited, abbreviated discovery process where Defendant has only a limited amount of time to conduct a document search and produce responsive documents. Defendant has interpreted this request as applying solely to the Office of the White House Press Secretary.

11. Defendants object to Instruction 1. Plaintiffs cite to no authority requiring a Defendant to “describe the efforts [it has] made to locate . . . document[s]” that are not in its custody and control “and identify who has control of the document and its location.”

12. Defendants object to Instruction 2 to the extent it exceeds the requirements of Fed. R. Civ. P. 26(b)(6). Defendants specifically decline to produce privileged information. Defendants further object to any requirement that they produce a privilege log for privileged material not otherwise properly within the scope of discovery or as to which no privilege log would be required under Federal Rule of Civil Procedure 26(b)(5).

13. Defendants object to Instruction 3. Plaintiffs cite to no authority indicating that, if Defendants object to an Interrogatory on burden grounds, Defendants must “stat[e] the approximate number of documents to be produced, the approximate number of person-hours to be incurred in the identification, and the estimated cost of responding to the request.” Further, it is unclear how Defendants could provide that type of information without conducting certain burdensome searches and reviews that Defendants sought to avoid through their objections.

14. Defendants object to Instruction 5 to the extent it requires Defendants to respond based on production of electronic documents “with all metadata and delivered in their original format.” Plaintiffs may identify the precise categories of metadata they want Defendants’ productions to contain, and Defendants can determine whether they can provide those categories of metadata without an undue burden.

15. Defendants object to Instruction 6 to the extent that it requires Defendants to

**CONFIDENTIAL**

**CONFIDENTIAL**

respond based on production of documents in a format other than the format in which they are “kept in the usual course of business.” Fed R. Civ. P. 34(b)(2)(E). Defendants object to Instruction 6 to the extent that it requests the production of all e-mail “forwards” for e-mails produced to Plaintiffs. That Instruction may call for the production of documents that are not found in the e-mail files of the relevant custodians used by Defendants.

16. Defendant objects to Instruction 8, which applies these requests to the Office of the White House Press Secretary from January 1, 2020, to the present, as unduly broad. Ms. Psaki served as White House Press Secretary from January 20, 2021, until May 13, 2022, when Ms. Jean-Pierre became White House Press Secretary. Defendant interprets these requests as applying to when Ms. Psaki served as White House Press Secretary from January 20, 2021, through May 13, 2022, and when Ms. Jean-Pierre began serving as White House Press Secretary until the date the requests were served, i.e., from May 13, 2022, to July 18, 2022. Anything else would be disproportional to the needs of the case. Such disproportionality is further aggravated by the discovery burden being placed on White House officials. *See Cheney v. U.S. District Court*, 542 U.S. 367, 385 (2004).

#### **GENERAL OBJECTIONS APPLICABLE TO ALL INTERROGATORIES**

1. The general objections set forth below apply to each and every Interrogatory discussed below. In asserting Defendants’ objections to any particular Interrogatory, Defendants may assert an objection that is the same as, or substantially similar to, one or more of these objections. That Defendants may refer, with particularity, to some, but not all, of the general objections described immediately below in their objections to Plaintiffs’ individual Interrogatories, does not indicate that Defendants have waived any of these general objections as to any of Plaintiffs’ Interrogatories.

**CONFIDENTIAL**

**CONFIDENTIAL**

2. Defendants object to any discovery taking place in this case to the extent Plaintiffs assert cognizable claims seeking review of governmental agency action, including claims under Administrative Procedure Act, because resolution of any such claims should be based upon the “administrative record” in this case. *See Fla. Power & Light Co. v. Lorion*, 470 U.S. 729, 743-44 (1985); *Citizens to Preserve Overton Park, Inc. v. Volpe*, 401 U.S. 402, 420 (1971). That said, Defendants understand that the Court has allowed preliminary-injunction-related expedited discovery to proceed. Thus, while preserving their broad objection to any and all discovery, Defendants make objections stated below in light of the current procedural posture of the case.

3. Defendants object to each Interrogatory insofar as it is directed to any Defendant that is head of a Defendant agency as overly broad, unduly burdensome, and disproportional in light of the extraordinarily expedited discovery schedule in this case, given that Plaintiffs have not first sought the information from the agency itself, or through alternative, less burdensome means. *See Fed. R. Civ. P. 26(b)(2)(C)*.

4. Defendants object to each Interrogatory as overbroad, unduly burdensome, and disproportional to the needs of the case, insofar as it purports to require a response from each agency concerning components of the agency or concerning governmental entities outside the agency whose actions are not challenged in the Complaint or Amended Complaint and whose information is not reasonably available to the agency or agency component whose alleged conduct is challenged in the Complaint or Amended Complaint. Defendant agencies include numerous components and employ thousands of individuals. Any construction of an Interrogatory that would require a Defendant agency to furnish information held by all such individuals, or require a Defendant agency to furnish information held by non-party agencies of the Federal Government, would be massively burdensome and disproportional to the needs of

**CONFIDENTIAL**



**CONFIDENTIAL**

this case. Each Defendant agency will identify appropriate individuals within the agency who will review and respond to each Interrogatory. *See, e.g., In re Epipen*, MDL No. 2785, 2018 WL 1440923, at \*2 (D. Kan. Mar. 15, 2018) (“[T]he party responding to discovery requests is typically in the best position to know and identify those individuals within its organization likely to have information relevant to the case.”).

5. Defendants object to the Interrogatories to the extent that they seek (a) attorney work product; (b) communications protected by the attorney-client privilege; (c) information protected by the deliberative process privilege or law enforcement privilege or other similar privilege; (d) material the disclosure of which would violate legitimate privacy interests and expectations of persons not party to this litigation; (e) information protected by any form of executive privilege; or (f) information covered by any other applicable privilege or protection.

6. Defendants object to any Interrogatory seeking discovery from the White House as unduly burdensome, and disproportional to the needs of the case. *See generally Cheney*, 542 U.S. at 367. Plaintiffs’ Interrogatories directed to White House officials would create an undue burden, distract them from their critical executive responsibilities, and violate the separation of powers. *See id.* at 385. That burden is especially undue at this stage of the litigation given that Defendants’ motion to dismiss the Amended Complaint for lack of subject-matter jurisdiction and other deficiencies is forthcoming. Further, the Interrogatories seeking response from the White House are unduly burdensome and disproportional to the needs of the case when Plaintiffs have not first exhausted all available opportunities to seek related information from other sources. *See Order, Centro Presente*, No. 1:18-cv-10340 (D. Mass. May 15, 2019) (requiring plaintiff to exhaust all discovery on other defendants before considering whether there was “continuing need for discovery sought on the White House”); *cf. Karnoski v. Trump*, 926 F.3d 1180, 1207 (9th Cir.

**CONFIDENTIAL**

**CONFIDENTIAL**

2019) (vacating “district court’s discovery orders because the district court did not fulfill its obligation ‘to explore other avenues, short of forcing the Executive to invoke privilege’” (quoting *Cheney*, 542 U.S. at 390)). Notwithstanding this objection, Defendants have amended their responses in a manner consistent with the Court’s September 6, 2022, Order.

7. Moreover, to the extent any Interrogatory a response requires review of information involving White House personnel, it is inappropriate because it may have the effect of seeking information protected by the presidential communications privilege, a “presumptive privilege” “fundamental to the operation of Government and inextricably rooted in the separation of powers under the Constitution” that attaches to presidential communications. *United States v. Nixon*, 418 U.S. 683, 708 (1974); see *In re Sealed Case*, 121 F.3d 729, 743-44 (D.C. Cir. 1997). Although the presidential communications privilege can be overcome by showing a “specific need” in a criminal case, *Judicial Watch, Inc. v. Dep’t of Justice*, 365 F.3d 1108, 1112 (D.C. Cir. 2004), the presumption against disclosure is even higher in a civil case like this one, *American Historical Ass’n v. Nat’l Archives & Records Admin.*, 402 F. Supp. 2d 171, 181 (D.D.C. 2005). Such discovery violates the separation of powers and creates an undue burden and distraction from those individuals’ critical executive responsibilities. See *Cheney*, 542 U.S. at 389.

8. Defendants object to each Interrogatory to the extent it seeks information or documents that are not in the custody or control of any Defendant.

9. Defendants object to each Interrogatory to the extent it seeks responses based on all communications and documents from each Defendant relating to the substantive topic identified in the Interrogatory. The parties are currently involved in an expedited, abbreviated discovery process in which Defendants have only a limited amount of time to respond.

10. Defendants specifically reserve the right to make further objections as necessary

**CONFIDENTIAL**

**CONFIDENTIAL**

to the extent additional issues arise regarding the meaning of and/or information sought by Plaintiffs' Interrogatories.

**PRELIMINARY STATEMENT REGARDING  
EXCESSIVELY NUMEROUS INTERROGATORIES**

1. Contrary to Fed. R. Civ. P. 33(a) and to LR33.1 of the Local Civil Rules, Plaintiffs erroneously and improperly served on July 18, 2022 First PI Interrogatories totaling 110 enumerated interrogatories as to 10 recipient Defendants. Even excluding duplicative interrogatories served on separate Defendants (at least in substance, if not form), there would still have been 34 distinct interrogatories.

2. Either number exceeds the 25 interrogatories permitted by the Federal Rules of Civil Procedure. *Global Tubing, LLC v. Tenaris Coiled Tubes, LLC*, No. 17-cv-3299, 2020 WL 12443175 at \*2 (S.D. Tex. Nov. 25, 2020) (quoting 8B Charles Alan Wright et al., *Federal Practice & Procedure* § 2168.1 (3d ed. 2020)); accord *Kleiman v. Wright*, No. 18-cv-80176, 2020 WL 1666787 at \*1 (S.D. Fla. Apr. 3, 2020); *Vinton v. Adam Aircraft Indus., Inc.*, 232 F.R.D. 650, 664 (D. Colo. 2005); see also *Zito v. Leasecomm Corp.*, 233 F.R.D. 395, 399 (S.D.N.Y. 2006); see, e.g., *Am. Council of Blind of Metro. Chi. v. Chi.*, No. 19-cv-6322, 2021 WL 5140475 at \*1-2 (N.D. Ill. Nov. 4, 2021); *Fair Housing Ctr. of Centr. Ind. v. Welton*, No. 18-cv-01098, 2019 WL 2422594 at \*5 (S.D. Ind. June 10, 2019). In a similar vein, LR33.1 of the Local Civil Rules, concerning "Number of Interrogatories," provides as follows (emphasis added): "No party shall serve on any other party *more than 25 interrogatories in the aggregate* without leave of court." Adherence to the 25-interrogatory limitation is especially appropriate at this stage of the instant action, where Defendants are already addressing extensive requests for production of documents ahead of the Rule 26 conference for the limited purpose of providing Plaintiffs with additional information concerning the already-filed application for a preliminary injunction. *Cf.*

**CONFIDENTIAL**

**CONFIDENTIAL**

*Gray v. Price*, No. 19-cv-10383, 2020 WL 12721645 at \*5 (E.D. Mich. Feb. 12, 2020).

3. After alerting Plaintiffs to this issue in an August 1, 2022, letter, and following additional e-mail correspondence with Plaintiffs, the parties agreed on August 11, 2022 to resolve the excessive numerosity problem as follows: Plaintiffs requested that (a) each Defendant recipient is to answer Interrogatories 1 through 5 of the First PI Interrogatories directed to CDC, with the reference to the CDC (in Interrogatory 1) to “be adjusted to refer to the recipient of the interrogatory,” and (b) certain Defendants are to answer additional interrogatories, totaling 20, specified by Plaintiffs, and Plaintiffs did not object to Defendants’ proposal that all remaining interrogatories be deemed withdrawn.

4. Defendants have set forth more fully below their objections and responses to the 5 “Common” and 20 “additional” Interrogatories specified by Plaintiff on August 11, 2022, and preserve all other objections with respect to all other Interrogatories served on July 18, 2022 (the “Withdrawn Interrogatories”), to the extent they are not deemed withdrawn. In particular, Defendants object to those Interrogatories as exceeding the numerical limit in FRCP 33(a) and LR33.1 of the Local Civil Rules.

### **SIGNATURES FOR RESPONSES**

1. Insofar as an Interrogatory is not objected to through the undersigned counsel, Defendants respond to them below, as amended and in accordance with the Court’s September 6, 2022 Order, with the signatures of the following (attached):

- a. For OSG: Max Lesko, Chief of Staff, OSG
- b. For NIAID: Jill R. Harper, Ph.D., Deputy Director for Science Management and Executive Officer, NIAID
- c. For CDC: Carol Crawford, Health Communications Specialist and Director,

**CONFIDENTIAL**

**CONFIDENTIAL**

Division of Digital Media, CDC

- d. For DHS: Samantha Vinograd, Acting Assistant Secretary of Homeland Security for Counterterrorism, Threat Prevention, and Law Enforcement Policy
- e. For CISA: Geoffrey Hale, Lead of Election Security & Resilience, CISA
- f. For the four HHS employees identified in the Court’s September 6, 2022 Order: Carol Maloney, Executive Officer/Deputy Agency Chief FOIA Officer, Office of the Assistant Secretary of Public Affairs
- g. For the White House Office of the Press Secretary: Robert E. Dornbush III, Chief of Staff and Special Assistant to the Press Secretary
- h. For Dr. Fauci, as Director of NIAID and Chief Medical Advisor to the President: Jill R. Harper, Ph.D., Deputy Director for Science Management and Executive Officer, NIAID

## **OBJECTIONS AND RESPONSES TO SPECIFIC INTERROGATORIES**

### **Common Interrogatory No. 1:**

**“Identify every officer, official, employee, staff member, personnel, contractor, or agent of” recipient Defendant “or any other federal official or agency who has communicated or is communicating with any Social-Media Platform regarding Content Modulation and/or Misinformation”**

**OBJECTIONS:** Defendants incorporate by reference the above objections. Defendants further object to this Interrogatory as overbroad, unduly burdensome, and not proportional to the needs of this case. This Interrogatory calls for identifying “personnel” or “contractor[s]” of any Defendant or any employee or subordinate of any Defendant who have communicated with any and all “Social-Media Platform[s],” even if those platforms are not at issue in the Complaint (or in

**CONFIDENTIAL**

**CONFIDENTIAL**

the Amended Complaint), and including each platform’s “officers, agents, employees, contractors, or any other person employed by or acting on behalf of [such] Social-Media Platform.” Defendants cannot conduct an exhaustive search to uncover all possible responsive information under the current, abbreviated expedited discovery schedule. Such expedited discovery is especially burdensome given that Defendants’ motion to dismiss the Amended Complaint for lack of subject-matter jurisdiction and other deficiencies is forthcoming. Defendants also object to the Interrogatory to the extent a response requires review of internal, deliberative documents discussing such communications, attorney client documents, or other privileged materials relating to agency communications. Defendants also object to this Interrogatory to the extent it seeks information protected by the deliberative process privilege, attorney-client privilege, law enforcement privilege, a statutory national security privilege, presidential communications privilege or any other applicable privilege. Additionally, challenges to administrative agency action are ordinarily not subject to discovery outside the administrative record. *Lorion*, 470 U.S. at 743-44. Moreover, this Interrogatory is overbroad, unduly burdensome, and disproportional to the needs of the case, insofar as it purports to require a response from each agency concerning components of the agency or concerning governmental entities outside the agency whose actions are not challenged in the Complaint or Amended Complaint and whose information is not reasonably available to the agency or agency component whose alleged conduct is challenged in the Complaint or Amended Complaint.

Further, Defendants object to this Interrogatory on the ground that any discovery on the White House at this stage of the litigation is unduly burdensome and disproportional to the needs of the case. Plaintiffs have not exhausted all other avenues of discovery before seeking discovery on the White House. *See, e.g.,* Order, *Centro Presente*, No. 1:18-cv-10340 (D. Mass. May 15,

**CONFIDENTIAL**

**CONFIDENTIAL**

2019); *Karnoski v. Trump*, 926 F.3d 1180, 1207 (9th Cir. 2019); *Cheney*, 542 U.S. at 390. Additionally, discovery propounded on White House officials would create an undue burden, distract them from their critical executive responsibilities, and violate the separation of powers. *See Cheney*, 542 U.S. at 385. That burden is especially undue at this stage of the litigation given that Defendants’ motion to dismiss the Amended Complaint for lack of subject-matter jurisdiction and other deficiencies is forthcoming. Additionally, Defendants object to this Interrogatory to the extent a response requires review of information protected by the presidential communications privilege or other executive privileges. *See Nixon*, 418 U.S. at 708. Additionally, Defendants object to this Interrogatory to the extent it is directed to information protected by the presidential communications privilege or other executive privileges. *See Nixon*, 418 U.S. at 708. Because Plaintiffs are not entitled to such information, the request imposes a burden on Defendant disproportionate to the minimal benefit (if any) that Plaintiffs might derive from the possibility of responsive, non-privileged information. *See Cheney*, 542 U.S. at 389.

Defendants further object to this Interrogatory as unreasonably cumulative and duplicative of Plaintiffs’ Requests for Production 2 and 3, in response to which Defendants are producing non-privileged e-mail communications between Defendants and employees of the “Social-Media Platforms” concerning Misinformation located within a review population consisting of e-mail files that (i) are collected from custodians who, having been identified through Defendants’ internal inquiry, are known to have communicated with employees of the Social-Media Platforms, and (ii) contain one or more reasonable search terms calculated to identify which of the communications identified in (i) relate to Misinformation. Those Requests for Production provide a more expeditious and significantly less burdensome method for Plaintiffs to obtain the information sought, considering the expedited nature of the discovery here and the broad scope of

**CONFIDENTIAL**

**CONFIDENTIAL**

this Interrogatory.

Additionally, Defendants object to this Interrogatory as overbroad and disproportional to the needs of the case, particularly in light of the expedited nature of the discovery, to the extent “communication” is meant to cover anything beyond e-mail exchanges. Defendants also object to the Interrogatory as overbroad and disproportional to the needs of the case to the extent it requests that responding agencies identify every individual who may have been included on any e-mail exchange, whether as sender or recipient or simply copied on the e-mail, between any Defendant and a social media company.

**RESPONSE:** Subject to and without waiving the above objections, Defendants provide the following responses, as amended in accordance with the Court’s September 6, 2022 Order, by Defendants, HHS, NIAID, CDC, DHS, CISA, White House Office of the Press Secretary, and Dr. Fauci in his role as Chief Medical Advisor to the President.

**HHS:**

**Four HHS employees identified in the Court’s September 6, 2022 Order:** Subject to and without waiving any of the foregoing objections, and based on a reasonable inquiry under the circumstances of abbreviated, expedited discovery, HHS refers to the documents being produced in response to Requests For Production 2 and 3, and states further that the custodians whose e-mails were collected are the following current and former HHS personnel, as required by the Court’s September 6, 2022 Order:

- Joshua Peck, Deputy Assistant Secretary for Public Engagement, Office of the Assistant Secretary for Public Affairs (ASPA)
- Tericka Lambert, former Director of Digital Engagement, COVID-19 Public Education Campaign, ASPA

**CONFIDENTIAL**



**CONFIDENTIAL**

- Janell Muhammad, former Deputy Director, COVID-19 Public Education Campaign, ASPA<sup>1</sup>
- Christy Choi, Deputy Director, Office of Communications, Health Resources and Services Administration (HRSA)

**OSG:** Subject to and without waiving the above objections, OSG refers to the documents being produced in response to Requests For Production 2 and 3, and states further that the custodians whose e-mails were collected include the following current and former OSG personnel:

- Dr. Vivek Murthy, U.S. Surgeon General
- Max Lesko, Chief of Staff
- Eric Waldo, Chief Engagement Officer for the U.S. Surgeon General
- Daniel Tartakovsky, Associate Director of Science and Policy
- Adam Beckman, Senior Advisor
- Ann Kim, Chief Innovation and Design Officer
- Kyla Fullenwider, Senior Advisor

**NIAID:** Subject to and without waiving the above objections, NIAID refers to the documents being produced in response to Requests For Production 2 and 3, and states further that the custodians whose e-mails were collected include the following current NIAID personnel:

- Anthony S. Fauci, M.D., Director, NIAID
- Courtney Billet, Director, Office of Communications and Government Relations, NIAID
- Jennifer Routh, Scientific Communications Editor, News and Science Writing Branch, Office of Communications and Government Relations, NIAID

---

<sup>1</sup> As of November 2021, Ms. Muhammad has served a different role in a different component of HHS. Nevertheless, her emails through July 18, 2022, were collected and reviewed.

**CONFIDENTIAL**

**CONFIDENTIAL**

- Kathy Stover, Chief, News and Science Writing Branch, Office of Communications and Government Relations, NIAID

**CDC:** Subject to and without waiving the above objections, CDC refers to the documents being produced in response to Requests For Production 2 and 3, and states further that the custodians whose e-mails were collected include the following current and former CDC personnel:

- Carol Crawford, Health Communications Specialist/Chief, Digital Media Branch
- Jay Dempsey, Health Communications Specialist
- Kate Galatas, Associate Deputy Director
- Ansley Hynes, Public Health Analyst
- Cynthia Jorgenson, Associate Director for Health Communications Science
- Tanya Hamburger, Health Communications Specialist
- Jessica Kolis, Health Communications Specialist
- Kathleen Layton, Health Communications Specialist
- Kristen Nordlund, Public Affairs Specialist
- Dagny Olivares, Supervisory Health Communications Specialist
- Jessica Schindelar, Health Communications Specialist
- Martha Sharan, Health Communications Specialist
- Lynn Sokler, Health Communications Specialist
- Dia Taylor, Deputy Chief Operating Officer
- Christopher Voegeli, Behavioral Scientist
- Elisabeth Wilhelm, Health Communications Specialist

**DHS:** Subject to and without waiving any of the foregoing objections, and based on a reasonable inquiry under the circumstances of abbreviated, expedited discovery, DHS refers to the documents being produced in response to Requests For Production 2 and 3, and states further that

**CONFIDENTIAL**

**CONFIDENTIAL**

the custodians whose e-mails were collected include the following current and former DHS personnel:

- Nina Jankowicz, former Executive Director of the DHS Disinformation Governance Board
- Robert Silvers, Under Secretary of Homeland Security for Strategy, Policy, and Plans
- Samantha Vinograd, Acting Assistant Secretary of Homeland Security for Counterterrorism and Threat Prevention
- John Cohen, former Assistant Secretary of Homeland Security for Counterterrorism and Threat Prevention
- Tamara Hutchinson, Director, Private Sector Engagement, Office of Intelligence and Analysis
- Hala Furst, Associate Director for Strategic Engagement, DHS Center for Prevention Programs and Partnerships
- Thomas McDermott, Acting Assistant Secretary of Homeland Security for Cyber, Infrastructure, Risk and Resilience
- Meghann Peterlin, former Acting Assistant Secretary of Homeland Security for Counterterrorism and Threat Prevention

**CISA:** CISA has identified the following custodians as having relevant communications, as produced in response to Requests For Production 2 and 3:

- Jen Easterly, Director, CISA
- Christopher Krebs, former Director, CISA
- Matthew Masterson, former Senior Election Lead, CISA

**CONFIDENTIAL**

**CONFIDENTIAL**

- Geoff Hale, Lead, Election Security and Resilience (ESR), National Risk Management Center (NRMC), CISA
- Brian Scully, Chief, Mis-, Dis-, and Malinformation (MDM) Team, NRMC, CISA
- Lauren Protentis, Engagements Lead, MDM Team, NRMC, CISA

In addition to the custodians identified above, CISA has identified the following current and former agency personnel as appearing in the communications produced in response to Plaintiffs' Requests For Production:

- Chad Josiah, Resilience Lead, MDM Team, NRMC, CISA
- Robert Schaul, Analysis and Response Lead, MDM Team, NRMC, CISA
- Alex Zaheer, Analyst, MDM Team, NRMC, CISA
- John Stafford, former Analyst, Countering Foreign Influence Task Force (CFITF) (which was the predecessor to the MDM team), NRMC, CISA

**White House Office of the Press Secretary:** Subject to and without waiving any of the foregoing objections, as amended in accordance with the Court's September 6, 2022, Order, and based on a reasonable inquiry under the circumstances of abbreviated, expedited discovery, the White House Office of the Press Secretary refers to the documents being produced in response to Requests For Production 2 and 3, and states further that the custodians whose e-mails were collected include the following current and former White House Office of Press Secretary personnel:

- Jennifer Psaki, in her official capacity as White House Press Secretary from January 20, 2021 to May 13, 2022.
- Karine Jean-Pierre, White House Office of the Press Secretary
- Kevin Munoz, White House Office of the Press Secretary

**CONFIDENTIAL**

**CONFIDENTIAL**

**White House Chief Medical Advisor:**

- Dr. Fauci does not have a White House email address, and no one at the White House reports to him. Thus, there were no emails to search. Therefore, for responsive documents related to Dr. Fauci, Defendants direct Plaintiffs to any documents already produced in response to Plaintiffs' requests as served on Dr. Fauci in his capacity as Director of NIAID. Those documents were located after a reasonable search of Dr. Fauci's NIAID email account and were produced without regard to whether Dr. Fauci was acting in his capacity as Director of NIAID or Chief Medical Advisor to the President.

**Common Interrogatory No. 2:**

**Identify all Communications with any Social-Media Platform relating to Content Modulation and/or Misinformation.**

**OBJECTIONS:** Defendants incorporate by reference the above objections. Defendants further object to this Interrogatory as overbroad, unduly burdensome, and not proportional to the needs of this case. This Interrogatory calls for information from any Defendant or any employee or subordinate of any Defendant, to any and all "Social-Media Platform[s]," even if those platforms are not at issue in the Complaint (or in the Amended Complaint), and including each platform's "officers, agents, employees, contractors, or any other person employed by or acting on behalf of [such] Social-Media Platform." Defendants cannot conduct an exhaustive search to uncover all possible responsive information under the current, abbreviated expedited discovery schedule. Such expedited discovery is especially burdensome given that Defendants' motion to dismiss the Amended Complaint for lack of subject-matter jurisdiction and other deficiencies is forthcoming. Defendants also understand this Interrogatory to seek only a response based on

**CONFIDENTIAL**

**CONFIDENTIAL**

communications between Defendants and third parties outside the government. To the extent that this Interrogatory seeks internal information referring to such communications, Defendants object to the Interrogatory as not proportional to the needs of the case, as it would require an extensive search of internal records that would not be possible to complete in the expedited period provided for current discovery and would be unnecessary in light of Defendants' agreement to produce the external communications themselves. Defendants also object to the Interrogatory to the extent a response requires review of internal, deliberative documents discussing such communications, attorney client documents, or other privileged materials relating to agency communications. Defendants also object to this Interrogatory to the extent it seeks information protected by the deliberative process privilege, attorney-client privilege, law enforcement privilege, a statutory national security privilege, presidential communications privilege, or any other applicable privilege. Additionally, challenges to administrative agency action are ordinarily not subject to discovery outside the administrative record. *Lorion*, 470 U.S. at 743-44. Moreover, this Interrogatory is overbroad, unduly burdensome, and disproportional to the needs of the case, insofar as it purports to require a response from each agency concerning components of the agency or concerning governmental entities outside the agency whose actions are not challenged in the Complaint or Amended Complaint and whose information is not reasonably available to the agency or agency component whose alleged conduct is challenged in the Complaint or Amended Complaint.

Further, Defendants object to this Interrogatory on the ground that any discovery on the White House at this stage of the litigation is unduly burdensome and disproportional to the needs of the case. Plaintiffs have not exhausted all other avenues of discovery before seeking discovery on the White House. *See, e.g.*, Order, *Centro Presente*, No. 1:18-cv-10340 (D. Mass. May 15,

**CONFIDENTIAL**

**CONFIDENTIAL**

2019); *Karnoski v. Trump*, 926 F.3d 1180, 1207 (9th Cir. 2019); *Cheney*, 542 U.S. at 390. Additionally, discovery propounded on White House officials would create an undue burden, distract them from their critical executive responsibilities, and violate the separation of powers. *See Cheney*, 542 U.S. at 385. That burden is especially undue at this stage of the litigation given that Defendants’ motion to dismiss the Amended Complaint for lack of subject-matter jurisdiction and other deficiencies is forthcoming. Additionally, Defendants object to this Interrogatory to the extent a response requires review of information protected by the presidential communications privilege or other executive privileges. *See Nixon*, 418 U.S. at 708. Because Plaintiffs are not entitled to such information, the request imposes a burden on Defendant disproportionate to the minimal benefit (if any) that Plaintiffs might derive from the possibility of responsive, non-privileged information. *See Cheney*, 542 U.S. at 389.

Additionally, Defendants object to this Interrogatory as overbroad and disproportional to the needs of the case, particularly in light of the expedited nature of the discovery, to the extent “communication” is meant to cover anything beyond e-mail exchanges.

Defendants further object to this Interrogatory as unreasonably cumulative and duplicative of Plaintiffs’ Requests for Production 2 and 3, in response to which Defendants are producing non-privileged e-mail communications between Defendants and employees of the Social-Media Platforms concerning Misinformation located within a review population consisting of e-mail files that (i) are collected from custodians who, having been identified through Defendants’ internal inquiry, are known to have communicated with employees of the Social-Media Platforms, and (ii) contain one or more reasonable search terms calculated to identify which of the communications identified in (i) relate to Misinformation. Those Requests for Production provide a more expeditious and significantly less burdensome method for Plaintiffs to obtain the information

**CONFIDENTIAL**

**CONFIDENTIAL**

sought, considering the expedited nature of the discovery here and the broad scope of this Interrogatory.

**RESPONSE:** Subject to and without waiving the above objections, Defendants provide the following responses, as amended in accordance with the Court's September 6, 2022 Order, by Defendants, HHS, NIAID, CDC, DHS, CISA, White House Office of the Press Secretary, and Dr. Fauci in his role as Chief Medical Advisor to the President:

Defendants refer Plaintiffs to the documents being produced in response to Plaintiffs' First Requests For Production to Defendants.

Further, in accordance with the Court's September 6, 2022 Order, subject to and without waiving any of the foregoing objections, and based on a reasonable inquiry under the circumstances of abbreviated, expedited discovery, including consultation with Dr. Fauci and review of Dr. Fauci and NIAID staff e-mail records, NIAID responds on behalf of Dr. Fauci in his role as Director of NIAID as follows: NIAID has not identified any communications, written or oral, between Dr. Fauci and Social-Media Platforms relating to Content Modulation and/or Misinformation. In general, Dr. Fauci has participated in media appearances and communications with or on Social-Media Platforms to publicize health information and provide COVID-19 and vaccine education, which are not responsive to this request. For an example, see NIAID's supplemental response to Additional Interrogatory 5, describing live interviews with Dr. Fauci and Mark Zuckerberg (CEO of Facebook) regarding COVID-19 and vaccines.

Defendants further note that Dr. Fauci does not have any responsive information in his role as Chief Medical Advisor beyond the information provided for Dr. Fauci in his role as Director of NIAID.

**CONFIDENTIAL**



**CONFIDENTIAL**

**Common Interrogatory No. 3:**

**Identify all Social-Media Platforms, including their officers, agents, or employees, with which You have communicated or are communicating with relating to Content Modulation and/or Misinformation.**

**OBJECTIONS:** Defendants incorporate by reference the above objections. Defendants further object to this Interrogatory as overbroad, unduly burdensome, and not proportional to the needs of this case. This Interrogatory calls for a response based on communications from any Defendant or any employee or subordinate of any Defendant, to any and all Social-Media Platforms, even if those platforms are not at issue in the Complaint (or in the Amended Complaint), and including each platform’s “officers, agents, employees, contractors, or any other person employed by or acting on behalf of [such] Social-Media Platform.” Defendants cannot conduct an exhaustive search to uncover all possible responsive information under the current, abbreviated expedited discovery schedule. Such expedited discovery is especially burdensome given that Defendants’ motion to dismiss the Amended Complaint for lack of subject-matter jurisdiction and other deficiencies is forthcoming. Defendants also object to this Interrogatory to the extent it seeks information protected by the deliberative process privilege, attorney-client privilege, law enforcement privilege, a statutory national security privilege, presidential communications privilege, or any other applicable privilege. Additionally, challenges to administrative agency action are ordinarily not subject to discovery outside the administrative record. *Lorion*, 470 U.S. at 743-44. Moreover, this Interrogatory is overbroad, unduly burdensome, and disproportional to the needs of the case, insofar as it purports to require a response from each agency concerning components of the agency or concerning governmental entities outside the agency whose actions are not challenged in the Complaint or Amended Complaint and whose information is not reasonably available to the agency or agency component whose alleged conduct is challenged in the Complaint or Amended Complaint.

**CONFIDENTIAL**

**CONFIDENTIAL**

Further, Defendants object to this Interrogatory on the ground that any discovery on the White House at this stage of the litigation is unduly burdensome and disproportional to the needs of the case. Plaintiffs have not exhausted all other avenues of discovery before seeking discovery on the White House. *See, e.g.,* Order, *Centro Presente*, No. 1:18-cv-10340 (D. Mass. May 15, 2019); *Karnoski v. Trump*, 926 F.3d 1180, 1207 (9th Cir. 2019); *Cheney*, 542 U.S. at 390. Additionally, discovery propounded on White House officials would create an undue burden, distract them from their critical executive responsibilities, and violate the separation of powers. *See Cheney*, 542 U.S. at 385. That burden is especially undue at this stage of the litigation given that Defendants’ motion to dismiss the Amended Complaint for lack of subject-matter jurisdiction and other deficiencies is forthcoming. Additionally, Defendants object to this Interrogatory to the extent a response requires review of information protected by the presidential communications privilege or other executive privileges. *See Nixon*, 418 U.S. at 708. Because Plaintiffs are not entitled to such information, the request imposes a burden on Defendant disproportionate to the minimal benefit (if any) that Plaintiffs might derive from the possibility of responsive, non-privileged information. *See Cheney*, 542 U.S. at 389.

Additionally, Defendants object to this Interrogatory as overbroad and disproportional to the needs of the case, particularly in light of the expedited nature of the discovery, to the extent “communication” is meant to cover anything beyond e-mail exchanges.

Defendants further object to this Interrogatory as unreasonably cumulative and duplicative of Plaintiffs’ Requests for Production 2 and 3, in response to which Defendants are producing non-privileged e-mail communications between Defendants and employees of the “Social-Media Platforms” concerning Misinformation located within a review population consisting of e-mail files that (i) are collected from custodians who, having been identified through Defendants’

**CONFIDENTIAL**

**CONFIDENTIAL**

internal inquiry, are known to have communicated with employees of the Social-Media Platforms, and (ii) contain one or more reasonable search terms calculated to identify which of the communications identified in (i) relate to Misinformation. Those Requests for Production provide a more expeditious and significantly less burdensome method for Plaintiffs to obtain the information sought, considering the expedited nature of the discovery here and the broad scope of this Interrogatory.

**RESPONSE:** Subject to and without waiving the above objections, Defendants provide the following responses, as amended in accordance with the Court's September 6, 2022 Order, by Defendants, HHS, NIAID, CDC, DHS, CISA, White House Office of the Press Secretary, and Dr. Fauci in his role as Chief Medical Advisor to the President:

Defendants refer Plaintiffs to the documents being produced in response to Plaintiffs' First Requests For Production to Defendants.

Further, in accordance with the Court's September 6, 2022 Order, subject to and without waiving any of the foregoing objections, and based on a reasonable inquiry under the circumstances of abbreviated, expedited discovery, including consultation with Dr. Fauci and review of Dr. Fauci and NIAID staff e-mail records, NIAID responds on behalf of Dr. Fauci in his role as Director of NIAID as follows: NIAID has not identified any communications, written or oral, between Dr. Fauci and Social-Media Platforms relating to Content Modulation and/or Misinformation. In general, Dr. Fauci has participated in media appearances and communications with or on Social-Media Platforms to publicize health information and provide COVID-19 and vaccine education, which are not responsive to this request. For an example, see NIAID's supplemental response to Additional Interrogatory 5, describing live interviews with Dr. Fauci and Mark Zuckerberg (CEO of Facebook) regarding COVID-19 and vaccines.

**CONFIDENTIAL**

**CONFIDENTIAL**

Defendants further note that Dr. Fauci does not have any responsive information in his role as Chief Medical Advisor beyond the information provided for Dr. Fauci in his role as Director of NIAID.

**Common Interrogatory No. 4:**

**Identify all meetings with any Social-Media Platform relating to Content Modulation and/or Misinformation.**

**OBJECTIONS:** Defendants incorporate by reference the above objections. Defendants further object that the Interrogatory is vague and ambiguous, including through the term “relating to . . . Misinformation.” Defendants further object to this Interrogatory as overbroad, unduly burdensome, and not proportional to the needs of this case. This Interrogatory calls for a response based on “meetings” by any Defendant or any employee or subordinate of any Defendant, with any and all Social-Media Platforms, even if those platforms are not at issue in the Complaint (or in the Amended Complaint), and including each platform’s “officers, agents, employees, contractors, or any other person employed by or acting on behalf of [such] Social-Media Platform.” Defendants cannot conduct an exhaustive search to uncover all possible responsive information under the current, abbreviated expedited discovery schedule. Such expedited discovery is especially burdensome given that Defendants’ motion to dismiss the Amended Complaint for lack of subject-matter jurisdiction and other deficiencies is forthcoming. Defendants also object to this Interrogatory to the extent it seeks information protected by the deliberative process privilege, attorney-client privilege, law enforcement privilege, a statutory national security privilege, presidential communications privilege, or any other applicable privilege. Additionally, challenges to administrative agency action are ordinarily not subject to discovery outside the administrative record. *Lorion*, 470 U.S. at 743-44. Moreover, this Interrogatory is overbroad, unduly burdensome,

**CONFIDENTIAL**

**CONFIDENTIAL**

and disproportional to the needs of the case, insofar as it purports to require a response from each agency concerning components of the agency or concerning governmental entities outside the agency whose actions are not challenged in the Complaint or Amended Complaint and whose information is not reasonably available to the agency or agency component whose alleged conduct is challenged in the Complaint or Amended Complaint.

Further, Defendants object to this Interrogatory on the ground that any discovery on the White House at this stage of the litigation is unduly burdensome and disproportional to the needs of the case. Plaintiffs have not exhausted all other avenues of discovery before seeking discovery on the White House. *See, e.g.,* Order, *Centro Presente*, No. 1:18-cv-10340 (D. Mass. May 15, 2019); *Karnoski v. Trump*, 926 F.3d 1180, 1207 (9th Cir. 2019); *Cheney*, 542 U.S. at 390. Additionally, discovery propounded on White House officials would create an undue burden, distract them from their critical executive responsibilities, and violate the separation of powers. *See Cheney*, 542 U.S. at 385. That burden is especially undue at this stage of the litigation given that Defendants' motion to dismiss the Amended Complaint for lack of subject-matter jurisdiction and other deficiencies is forthcoming. Additionally, Defendants object to this Interrogatory to the extent a response requires review of information protected by the presidential communications privilege or other executive privileges. *See Nixon*, 418 U.S. at 708. Because Plaintiffs are not entitled to such information, the request imposes a burden on Defendant disproportionate to the minimal benefit (if any) that Plaintiffs might derive from the possibility of responsive, non-privileged information. *See Cheney*, 542 U.S. at 389.

Defendants further object to this Interrogatory as unreasonably cumulative and duplicative of Plaintiffs' Requests for Production 2, 3, and 4, in response to which Defendants are producing non-privileged e-mail communications between Defendants and employees of the Social-Media

**CONFIDENTIAL**

**CONFIDENTIAL**

Platforms concerning Misinformation located within a review population consisting of e-mail files that (i) are collected from custodians who, having been identified through Defendants' internal inquiry, are known to have communicated with employees of the Social-Media Platforms, and (ii) contain one or more reasonable search terms calculated to identify which of the communications identified in (i) relate to Misinformation. Those Requests for Production provide a more expeditious and significantly less burdensome method for Plaintiffs to obtain the information sought, considering the expedited nature of the discovery here and the broad scope of this Interrogatory.

**RESPONSE:** Subject to and without waiving the above objections, Defendants provide the following responses, as amended and in accordance with the Court's September 6, 2022 Order, by Defendants, HHS, NIAID, CDC, DHS, CISA, White House Office of the Press Secretary, and Dr. Fauci in his role as Chief Medical Advisor to the President:

**HHS.** Subject to and without waiving any of the foregoing objections, and based on a reasonable inquiry under the circumstances of abbreviated, expedited discovery, HHS has identified OSG, NIAID, and CDC as available sources of information that is potentially responsive to Plaintiffs' discovery requests. HHS directs Plaintiffs to those agencies' responses. Defendants have also amended their responses for the four HHS officials identified in the Court's September 6, 2022 Order.

**Four HHS employees identified in the Court's September 6, 2022 Order:** Subject to and without waiving any of the foregoing objections, and based on a reasonable inquiry under the circumstances of abbreviated, expedited discovery, HHS responds as follows based on the knowledge of the four HHS employees identified in the Court's September 6, 2022 Order:

HHS has specifically identified three meetings where misinformation was discussed:

**CONFIDENTIAL**

**CONFIDENTIAL**

- On March 1, 2021, from 2:00 to 2:30 pm ET, there was a virtual meeting attended by Joshua Peck and Twitter personnel. Besides Mr. Peck, the invitees included: Robert Flaherty, Clarke Humphrey, Benjamin Wakana, Courtney Rowe, Todd O'Boyle, and Lauren Culbertson.
- On March 1, 2021, from 3:00 to 3:30 pm ET, there was a virtual meeting attended by Joshua Peck and Facebook personnel. Besides Mr. Peck, the invitees included: Robert Flaherty, Clarke Humphrey, Courtney Rowe, Payton Itheme, Brian Rice, Carrie Adams, Genelle Adrien, and Julia Eisman. It is also possible that Andrew Slavitt attended.
- As indicated by MOLA\_DEFSPROD\_00007398, on November 22, 2021, from 4:00 to 4:30 pm ET, there was a virtual meeting attended by Tericka Lambert, other ASPA personnel, personnel from Fors Marsh Group (a contractor for ASPA), personnel from OSG, and Google/YouTube personnel. This meeting briefly touched on misinformation among other topics.

Additionally, HHS has identified various meetings with some social media platforms to discuss HHS's COVID-19 public-education efforts, in which Ms. Lambert, Mr. Peck, and Ms. Muhammad were involved. Misinformation was not the focal point of the meetings, but it is possible that misinformation was mentioned. For instance, the meetings may have mentioned misinformation to the extent it related to strategies to promote HHS COVID-19 public-education content. HHS has not identified any meetings with social media platforms in which Ms. Choi was involved.

**OSG.** Subject to and without waiving any of the foregoing objections, and based on a reasonable inquiry under the circumstances of abbreviated, expedited discovery, OSG responds

**CONFIDENTIAL**

**CONFIDENTIAL**

that the following meetings took place with the Social-Media Platforms relating to Misinformation:

- On July 12, 2021, from 3:00 pm to 3:30 pm ET, Eric Waldo from OSG met remotely with Lauren Culberton and Todd Boyle from Twitter. Kyla Fullenwider from U.S. Digital Response was invited and may have also attended. The meeting provided notice of the upcoming OSG Advisory and a high-level view of what issues OSG would be prioritizing in the Advisory.
- On July 14, 2021, from 3:00 pm to 3:30 pm ET, Eric Waldo from OSG met remotely with Kevin Kane from YouTube, Jan Antonaros from Google, and Ariel Altman from YouTube. The meeting provided notice of the upcoming OSG Advisory and a high-level view of what issues OSG would be prioritizing in the Advisory.
- On July 16, 2021, from 3:00 pm to 3:30 pm ET, Eric Waldo from OSG and Kyla Fullenwider from U.S. Digital Response met remotely with Payton Itheme and Justine Isola from Facebook. Kate Thornton and Brian Rice from Facebook were invited and may have also attended. The meeting discussed the newly issued OSG Advisory.
- On July 23, 2021, from 1:30 pm to 2:00 pm ET, Dr. Vivek Murthy and Eric Waldo from OSG, and D.J. Patil (who OSG understands to be a then part-time consultant supporting the Office of Science Technology and Policy) met remotely with Nick Clegg and (very likely) Brian Rice from Facebook. The meeting discussed a recent e-mail from Mr. Clegg to Dr. Murthy concerning recent public comments by the Administration about Facebook.
- On July 30, 2021, from 2:00 pm to 2:30 pm ET, Eric Waldo from OSG met with Kevin Kane from YouTube, Lauren Kelly from Google, and Jan Antonaros from Google. The

**CONFIDENTIAL**



**CONFIDENTIAL**

topics discussed included YouTube/Google following up on the announcement of the OSG Advisory to share more of the work it was doing around health mis- and disinformation.

- As indicated by MOLA\_DEFSPROD\_00007398, on November 22, 2021, from 4:00 to 4:30 pm ET, there was a virtual meeting attended by Tericka Lambert, other ASPA personnel, personnel from Fors Marsh Group (a contractor for ASPA), personnel from OSG, and Google/YouTube personnel. This meeting briefly touched on misinformation among other topics.

**NIAID.** Subject to and without waiving any of the foregoing objections, and based on a reasonable inquiry under the circumstances of abbreviated, expedited discovery, NIAID responds that no meetings took place with the Social-Media Platforms relating to Misinformation. NIAID has identified two possible meetings to discuss the potential participation by the NIAID director in U.S. Government efforts to publicize health information and provide COVID-19 and vaccine education via social media, which are not responsive to the Interrogatory, but are identified in the documents being produced in response to Plaintiffs' First Requests For Production to Defendants:

- Facebook approached NIAID in March 2020 to discuss public service announcements and ads, Facebook's CV19 hub, and an interview between Dr. Fauci and Mark Zuckerberg; NIAID scheduled the interview between Dr. Fauci and Mr. Zuckerberg (which aired on Facebook Live)
- NIAID was invited to, but did not attend, a meeting scheduled for March 4, 2021, to discuss possible Facebook Live interviews with celebrities/influencers related to COVID-19 vaccines

**CONFIDENTIAL**

**CONFIDENTIAL**

Further, in accordance with the Court’s September 6, 2022 Order, subject to and without waiving any of the foregoing objections, and based on a reasonable inquiry under the circumstances of abbreviated, expedited discovery, including consultation with Dr. Fauci and review of Dr. Fauci and NIAID staff e-mail records, NIAID responds on behalf of Dr. Fauci in his role as Director of NIAID as follows: NIAID has not identified any communications, written or oral, with the Social-Media Platforms and Dr. Fauci relating to Content Modulation and/or Misinformation. In general, Dr. Fauci has participated in media appearances and communications with or on Social-Media Platforms to publicize health information and provide COVID-19 and vaccine education, which are not responsive to this request. For an example, see NIAID’s supplemental response to Additional Interrogatory 5, describing live interviews with Dr. Fauci and Mark Zuckerberg (CEO of Facebook) regarding COVID-19 and vaccines.

**CDC.** Subject to and without waiving any of the foregoing objections, and based on a reasonable inquiry under the circumstances of abbreviated, expedited discovery, CDC responds that the following meetings took place with the Social-Media Platforms relating to Misinformation:

- On May 14, 2021, and May 28, 2021, there were virtual “Be on the Lookout” meetings concerning certain items of developing and prevalent COVID-19 misinformation on social media. The invitees included: Todd O’Boyle from Twitter; Stanley Onyimba, Jan Antonaros, and Kevin Kane from Google; Payton Iheme, Liz Lagone, Lexi Sturdy, and Carrie Adams from Facebook; Sam Huxley from Reingold; Christopher Thomas Lewitzke, Caroline Faught, and Jennifer Shopkorn from the United States Census Bureau (“Census”); and Lynn Sokler, Carol Crawford, and Kate Galatas from CDC.

**CONFIDENTIAL**

**CONFIDENTIAL**

- On February 4, 2021 and February 25, 2021 there were virtual or telephonic meetings during which it is likely that misinformation was discussed among other topics. The invitees included: Payton Itheme, Chelsey Lepage, Genelle Adrien, Airton Tatoug Kamdem, Julia Eisman, Liz Lagone, Kate Thornton, and Carrie Adams from Facebook; and Kathleen Layton, Jay H. Dempsey, and Carol Crawford from CDC.
- On March 18, 2021, there was a virtual or telephonic meeting during which it is likely that misinformation was discussed among other topics. The invitees included: Payton Itheme, Chelsey Lepage, Genelle Adrien, Airton Tatoug Kamdem, Julia Eisman, Liz Lagone, Kate Thornton, and Carrie Adams from Facebook; Georgeta Dragiou and Stacey Palosky from the Office of the Assistant Secretary of Public Affairs within HHS; and Kathleen Layton, Jay H. Dempsey, and Carol Crawford from CDC.
- On March 25, 2021, there was a virtual or telephonic meeting to discuss misinformation. The invitees included Payton Itheme, Priya Gangolly, Chelsey Lepage, Genelle Adrien, Justine Isola, Lindsay Young, Sunita Saligram, Airton Tatoug Kamdem, Nisha Deolalikar, Julia Eisman, Athas Nikolakos, Liz Lagone, Stephanie Bousheri, Kate Thornton, and Carrie Adams from Facebook; and Kathleen Layton, Jay H. Dempsey, and Carol Crawford from CDC.
- On May 13, 2021, there was a virtual or telephonic meeting during which it is likely that misinformation was discussed among other topics. The invitees included: Payton Itheme, Chelsey Lepage, Genelle Adrien, Sadie Pulliam, Airton Tatoug Kamdem, Julia Eisman, Liz Lagone, Kate Thornton, and Carrie Adams from Facebook; and Kathleen Layton, Jay H. Dempsey, and Carol Crawford from CDC.
- On May 19, 2021, there was a virtual meeting to provided training on Facebook's

**CONFIDENTIAL**

**CONFIDENTIAL**

- channel for reporting misinformation. The invitees included: Kathleen Layton, Carol Crawford, Lynn Sokler, Kate Galatas, Brooke Aspinwall, and Jay Dempsey from CDC; Christopher Lewitzke, Sam Huxley, and Kathleen Stanley from Reingold; Carrie Adams from Facebook; and Jennifer Shopkorn, Michelle Christine O'Malley, and Caroline Faught from Census.
- On May 20, 2021, there was a virtual or telephonic meeting during which it is likely that misinformation was discussed among other topics. The invitees included: Payton Itheme, Chelsey Lepage, Genelle Adrien, Cariza Arnedo, Airton Tatoug Kamdem, Julia Eisman, Liz Lagone, Kate Thornton, and Carrie Adams from Facebook; Kathleen Layton, Jay H. Dempsey, Cynthia Jorgenson, and Carol Crawford from CDC; and Sam Huxley from Reingold.
  - On August 31, 2021, there was a virtual meeting to discuss misinformation, including misinformation related to the Vaccine Adverse Event Reporting System (VAERS). The invitees included: Elaine Miller, Pedro Moro, Kristen Nordlund, Martha Sharan, John Su, Catherine Jamal, Stephanie Gordon, Jessica Schindelar, Lynn Sokler, Alexis Hauk, Tanya Hamburger, and Carol Crawford from CDC; and Carrie Adams from Facebook.
  - On March 24, 2021, there was a virtual meeting to discuss misinformation with Google/YouTube. The invitees included: Stanley Onyimba, Jan Antonaros, Scott Deutchman, Kevin Kane, and Clement Wolf from Google; Zachary Henry Schwartz and Jennifer Shopkorn from Census; Christopher Lewitzke and Sam Huxley from Reingold; and Carol Crawford, Lynn Sokler, Kate Galatas, Jessica Kolis, and Kathleen LaPorte from CDC.
  - On March 29, 2022, there was a virtual meeting with Google during which it is likely

**CONFIDENTIAL**

**CONFIDENTIAL**

that misinformation was discussed among other topics. The invitees included: Stanley Onyimba and Jan Antonaros from Google; and Fred Smith and Carol Crawford from CDC.

- On March 31, 2021, there was a virtual meeting with Twitter to discuss COVID-19 misinformation. The invitees included: Zachary Schwartz and Jennifer Shopkorn, from Census; Christopher Lewitzke and Sam Huxley from Reingold; Lynn Sokler, Kate Galatas, Rosemary Bretthauer-Mueller, Jessica Kolis, Kathleen LaPorte, and Carol Crawford from CDC; and Todd O’Boyle and Reggie McCrimmon from Twitter.
- On November 18, 2021, there was a meeting with Twitter to discuss VAERS as it related to misinformation. The invitees included: Todd O’Boyle, Brian Clark, Rodrigo Rianza Perez, and Joseph Guay from Twitter; and Carol Crawford, John Su, Alexis Hauk, Alanna Moorer, Nicole Coffin, Martha Sharan, Jessica Schindelar, and Jade Fulce from CDC.

**DHS** Subject to and without waiving any of the foregoing objections, and based on a reasonable inquiry under the circumstances of abbreviated, expedited discovery, DHS responds that meetings taking place with the Social-Media Platforms relating to Misinformation include, but are not limited to:

- A recurring meeting usually entitled USG – Industry meeting, which has generally had a monthly cadence, and is between government agencies and private industry. Government participants have included CISA’s Election Security and Resilience team, DHS’s Office of Intelligence and Analysis, the FBI’s foreign influence task force, the Justice Department’s national security division, and the Office of the Director of

**CONFIDENTIAL**

**CONFIDENTIAL**

National Intelligence. Industry participants have included Google, Facebook, Twitter, Reddit, Microsoft, Verizon Media, Pinterest, LinkedIn and the Wikimedia Foundation. The topics discussed include, but are not limited to: information sharing around elections risk, briefs from industry, threat updates, and highlights and upcoming watch outs.

- CISA Cybersecurity Advisory Committee (CSAC) Meetings on December 10, 2021; March 31, 2022; and June 22, 2022. The meeting agendas and summaries, including participants, are available on CISA’s website, <https://www.cisa.gov/cisa-cybersecurity-advisory-committee-meeting-resources>.
- Additional meetings identified in documents, include, but are not limited to:

<b>Date</b>	<b>Title</b>
7/20/20	ASD-HKS Tech Policy Paper Series: Levers in the Online Ad Ecosystem
1/18/22	Google + Digital Forum
3/16/22	DHS/Microsoft Disinformation Follow Up
2/1/22	Meta/DHS/DOJ Engagement re: Human Trafficking

**CISA:** Subject to and without waiving any of the foregoing objections, and based on a reasonable inquiry under the circumstances of abbreviated, expedited discovery, CISA responds that meetings taking place with the Social-Media Platforms relating to Misinformation include, but are not limited to:

- A recurring meeting usually entitled USG – Industry meeting, which has generally had a monthly cadence, and is between government agencies and private industry. Government participants have included CISA’s Election Security and Resilience subdivision, DHS’s Office of Intelligence and Analysis, the FBI’s foreign influence task force, the Justice Department’s national security division, and the Office of the Director of National Intelligence. Industry participants generally include Google, Facebook, Twitter, Reddit,

**CONFIDENTIAL**

**CONFIDENTIAL**

Microsoft but, have also included Verizon Media, Pinterest, LinkedIn, and the Wikimedia Foundation as well. The topics discussed include, but are not limited to: information sharing around elections risk, briefs from industry, threat updates, and highlights and upcoming watch outs.

- A recurring meeting to prepare for and set the agenda for the USG – Industry meeting, and participants have generally included CISA and Facebook.
- CISA Cybersecurity Advisory Committee (CSAC) Meetings on December 10, 2021; March 31, 2022; and June 22, 2022. The meeting agendas and summaries, including participants, are available on CISA’s website, <https://www.cisa.gov/cisa-cybersecurity-advisory-committee-meeting-resources>.
- CISA CSAC, Protecting Critical Infrastructure from Misinformation and Disinformation Subcommittee meetings. The Subcommittee was established for the purpose of evaluating and providing recommendations on potentially effective critical infrastructure related counter-MDM efforts that fit within CISA’s unique capabilities and mission. Details about the Subcommittee, including membership, are available on CISA’s website, [https://www.cisa.gov/sites/default/files/publications/CSAC\\_Subcommittee\\_Fact\\_Sheet\\_05192022\\_508c.pdf](https://www.cisa.gov/sites/default/files/publications/CSAC_Subcommittee_Fact_Sheet_05192022_508c.pdf).
- Meetings convened by the Election Infrastructure Subsector Government Coordinating Council (EIS-GCC) and Election Infrastructure Subsector Coordinating Council (EI-SCC) Joint MDM Working Group. The Joint MDM Working Group was launched after the 2020 election by the EIS-GCC and EI-SCC and provides a forum through which the subsector can identify challenges in countering MDM and produce resources for addressing such challenges. The Joint MDM Working Group has convened meetings on, or about May 5,

**CONFIDENTIAL**

**CONFIDENTIAL**

2021; June 7, 2021; September 14, 2021; November 19, 2021, June 30, 2022, and August 4, 2022.

**White House Office of the Press Secretary:** Subject to and without waiving any of the foregoing objections, and based on a reasonable inquiry under the circumstances of abbreviated, expedited discovery, the White House Office of the Press Secretary provides the following response: The White House Office of the Press Secretary (“the Office”) is unaware of any meetings involving the Office and a social media company concerning content modulation or misinformation.

**White House Chief Medical Advisor:** Further, subject to and in accordance with the Court’s September 6, 2022 Order, for Dr. Fauci in his role as Director of NIAID, Defendants provide the following additional response, subject to and without waiving any of the foregoing objections: Defendants aver that Dr. Fauci does not have any responsive information in his role as Chief Medical Advisor beyond the information provided for Dr. Fauci in his role as Director of NIAID.

**Common Interrogatory No. 5:**

**Identify all Communications with any Social-Media Platform that contain any of the Search Term(s).**

**OBJECTIONS:** Defendants incorporate by reference the above objections. Defendants further object to this Interrogatory as unduly burdensome, overbroad, and not proportional to the needs of this case. This Interrogatory calls for a response based on any and all specified documents from any Defendant or any employee or subordinate of any Defendant. Defendants cannot conduct an exhaustive search to uncover all possible responsive information under the current, abbreviated expedited discovery schedule. Such expedited discovery is especially burdensome given that Defendants’ motion to dismiss the Amended Complaint for lack of subject-matter jurisdiction and other deficiencies is forthcoming. Furthermore, this Interrogatory covers documents that are not

**CONFIDENTIAL**



**CONFIDENTIAL**

relevant to Plaintiffs' claims and that do not fall within scope of discovery authorized by the Court. The Court authorized the service of discovery requests concerning "the identity of federal officials who have been and are communicating with social-media platforms about [misinformation and] any censorship or suppression of speech on social media, including the nature and content of those communications." ECF No. 34 at 13. This Interrogatory, however, seeks information that contains any of Plaintiffs' Search Terms, regardless of whether that document pertains to Misinformation. Plaintiffs' Search Terms include many broad terms that could be found in e-mails that have nothing to do with misinformation—such as "mask," "election," "antitrust," "globalization," and "Federalist." Defendants also understand this Interrogatory to seeks a response based on only communications between Defendants and third parties outside the government. To the extent that this Interrogatory seeks internal information referring to such communications, Defendants object to the Interrogatory as not proportional to the needs of the case, as it would require an extensive search of internal records that would not be possible to complete in the expedited period provided for current discovery and would be unnecessary in light of Defendants' agreement to produce the external communications themselves. Defendants also object to the Interrogatory to the extent a response requires review of internal, deliberative documents discussing such communications, attorney client documents, or other privileged materials relating to agency communications. Defendants also object to this Interrogatory to the extent it seeks information protected by the deliberative process privilege, attorney-client privilege, law enforcement privilege, a statutory national security privilege, presidential communications privilege, or any other applicable privilege. Additionally, challenges to administrative agency action are ordinarily not subject to discovery outside the administrative record. *Lorion*, 470 U.S. at 743-44. Moreover, this Interrogatory is overbroad, unduly burdensome, and disproportional to the needs of the case,

**CONFIDENTIAL**

**CONFIDENTIAL**

insofar as it purports to require a response from each agency concerning components of the agency or concerning governmental entities outside the agency whose actions are not challenged in the Complaint or Amended Complaint and whose information is not reasonably available to the agency or agency component whose alleged conduct is challenged in the Complaint or Amended Complaint.

Further, Defendants object to this Interrogatory on the ground that any discovery on the White House at this stage of the litigation is unduly burdensome and disproportional to the needs of the case. Plaintiffs have not exhausted all other avenues of discovery before seeking discovery on the White House. *See, e.g.,* Order, *Centro Presente*, No. 1:18-cv-10340 (D. Mass. May 15, 2019); *Karnoski v. Trump*, 926 F.3d 1180, 1207 (9th Cir. 2019); *Cheney*, 542 U.S. at 390. Additionally, discovery propounded on White House officials would create an undue burden, distract them from their critical executive responsibilities, and violate the separation of powers. *See Cheney*, 542 U.S. at 385. That burden is especially undue at this stage of the litigation given that Defendants' motion to dismiss the Amended Complaint for lack of subject-matter jurisdiction and other deficiencies is forthcoming. Additionally, Defendants object to this Interrogatory to the extent a response requires review of information protected by the presidential communications privilege or other executive privileges. *See Nixon*, 418 U.S. at 708. Because Plaintiffs are not entitled to such information, the request imposes a burden on Defendant disproportionate to the minimal benefit (if any) that Plaintiffs might derive from the possibility of responsive, non-privileged information. *See Cheney*, 542 U.S. at 389.

Additionally, Defendants object to this Interrogatory as overbroad and disproportional to the needs of the case, particularly in light of the expedited nature of the discovery, to the extent "communication" is meant to cover anything beyond e-mail exchanges.

**CONFIDENTIAL**

**CONFIDENTIAL**

Defendants further object to this Interrogatory as unreasonably cumulative and duplicative of Plaintiffs' Requests for Production 2 and 3, in response to which Defendants are producing non-privileged e-mail communications between Defendants and employees of the "Social-Media Platforms" concerning Misinformation located within a review population consisting of e-mail files that (i) are collected from custodians who, having been identified through Defendants' internal inquiry, are known to have communicated with employees of the Social-Media Platforms, and (ii) contain one or more reasonable search terms calculated to identify which of the communications identified in (i) relate to Misinformation. Those Requests for Production provide a more expeditious and significantly less burdensome method for Plaintiffs to obtain the information sought, considering the expedited nature of the discovery here and the broad scope of this Interrogatory.

**RESPONSE:**

Subject to and without waiving the above objections, Defendants provide the following responses, as amended in accordance with the Court's September 6, 2022 Order, by Defendants, HHS, NIAID, CDC, DHS, CISA, White House Office of the Press Secretary, and Dr. Fauci in his role as Chief Medical Advisor to the President: Defendants refer Plaintiffs to the documents being produced in response to Plaintiffs' First Requests For Production to Defendants.

**Additional Interrogatory No. 1 (HHS No. 6):**

**Identify all "members of our senior staff" and/or "members of our COVID-19 team" who are "in regular touch with ... social media platforms," as Jennifer Psaki stated at a White House press briefing on or around July 15, 2021, including all Communications relating to such coordination.**

**OBJECTIONS:** Defendants incorporate by reference the above objections. Defendants further object to this Interrogatory as vague because it relies on a characterization of a statement made by an individual no longer in government, and the statement does not specify the individuals

**CONFIDENTIAL**

**CONFIDENTIAL**

at issue or the specific communications referred to. Defendants also object to this Interrogatory to the extent it seeks information protected by the deliberative process privilege, attorney-client privilege, law enforcement privilege, a statutory national security privilege, or any other applicable privilege. Additionally, challenges to administrative agency action are ordinarily not subject to discovery outside the administrative record. *Lorion*, 470 U.S. at 743-44. Moreover, this Interrogatory is overbroad, unduly burdensome, and disproportionate to the needs of the case, insofar as it purports to require a response concerning components of the agency or concerning governmental entities outside the agency whose actions are not challenged in the Complaint or Amended Complaint and whose information is not reasonably available to the agency or agency component whose alleged conduct is challenged in the Complaint or Amended Complaint.

Additionally, Defendants object to this Interrogatory as overbroad and disproportional to the needs of the case, particularly in light of the expedited nature of the discovery, to the extent “communication” is meant to cover anything beyond e-mail exchanges.

Further, Defendant objects to this Interrogatory as unreasonably cumulative and duplicative of Common Interrogatories 1 through 5. Defendants otherwise refer Plaintiffs to the documents being produced with these responses for any additional information.

**RESPONSE:** Subject to and without waiving the above objections, as amended in accordance with the Court’s Order of September 6, 2022, Defendants provide the following responses for Defendant HHS, responding through OSG, NIAID, CDC, and for the four HHS employees identified in the Court’s September 6, 2022 Order, each of which refers to its response to Common Interrogatories 1 through 5 and the accompanying documents, *see generally* Fed. R. Civ. P. 33(d).

**Additional Interrogatory No. 2 (HHS No. 7):**

**CONFIDENTIAL**

**CONFIDENTIAL**

**Identify all Communications with any Social-Media Platform relating to the “12 people who are producing 65 percent of anti-vaccine misinformation on social media platform,” as stated by Jennifer Psaki at the July 15, 2021 press briefing.**

**OBJECTIONS:** Defendants incorporate by reference the above objections. Defendants further object to this Interrogatory as vague because it relies on a characterization of a statement made by an individual no longer in government, and the statement does not specify the individuals at issue or the specific communications referred to. Defendants also object to this Interrogatory to the extent it seeks information protected by the deliberative process privilege, attorney-client privilege, law enforcement privilege, a statutory national security privilege, or any other applicable privilege. Additionally, challenges to administrative agency action are ordinarily not subject to discovery outside the administrative record. *Lorion*, 470 U.S. at 743-44. Moreover, this Interrogatory is overbroad, unduly burdensome, and disproportionate to the needs of the case, insofar as it purports to require a response concerning components of the agency or concerning governmental entities outside the agency whose actions are not challenged in the Complaint or Amended Complaint and whose information is not reasonably available to the agency or agency component whose alleged conduct is challenged in the Complaint or Amended Complaint.

Additionally, Defendants object to this Interrogatory as overbroad and disproportional to the needs of the case, particularly in light of the expedited nature of the discovery, to the extent “communication” is meant to cover anything beyond e-mail exchanges.

Further, Defendant objects to this Interrogatory as unreasonably cumulative and duplicative of Common Interrogatories 1 through 5. Defendants otherwise refer Plaintiffs to the documents being produced with these responses for any additional information.

**RESPONSE:** Subject to and without waiving any of the foregoing objections, and based on a reasonable inquiry under the circumstances of the abbreviated, expedited discovery, HHS has identified OSG and CDC as available sources of information that is potentially responsive to this

**CONFIDENTIAL**

**CONFIDENTIAL**

Interrogatory. In accordance with the Court’s September 6, 2022, Order, HHS responds as follows on behalf of the four HHS identified by the Court: HHS refers to its response to Common Interrogatories 1 through 5 and the accompanying documents. *See generally* Fed. R. Civ. P. 33(d).

**OSG.** Subject to and without waiving the above objections, and based on a reasonable inquiry under the circumstances of abbreviated, expedited discovery, OSG refers to its response to Common Interrogatories 1 through 5 and the accompanying documents. *See generally* Fed. R. Civ. P. 33(d).

**CDC.** Subject to and without waiving the above objections, and based on a reasonable inquiry under the circumstances of abbreviated, expedited discovery, CDC refers to its response to Common Interrogatories 1 through 5 and the accompanying documents. *See generally* Fed. R. Civ. P. 33(d).

**Additional Interrogatory No. 3 (HHS No. 8):**

**Identify all “government experts” who are federal officers, officials, agents, employees, or contractors, who have “partnered with” Facebook or any other Social-Media Platform to address Misinformation and/or Content Modulation, including all Communications between such “government expert(s)” and any Social-Media Platform.**

**OBJECTIONS:** Defendants incorporate by reference the above objections. Defendants further object to this Interrogatory as vague because it relies on a characterization of a statement attributed to a third-party Facebook, as reported in a July 15, 2021 *Reuters.com* article quoted at Compl. ¶ 163, and the statement does not sufficiently specify the individuals at issue or the specific communications referred to. Defendants lack information sufficient to establish the meaning of that third party’s statement, including terms such as “partnered with.” Defendants further object to this Interrogatory as unduly burdensome and not proportional to the needs of the case. Defendants cannot conduct an exhaustive search to uncover all possible responsive information under the

**CONFIDENTIAL**

**CONFIDENTIAL**

current, abbreviated expedited discovery schedule. Such expedited discovery is especially burdensome given that Defendants' motion to dismiss the Amended Complaint for lack of subject-matter jurisdiction and other deficiencies is forthcoming. Defendants also object to the Interrogatory to the extent a response requires review of internal, deliberative documents discussing such communications, attorney client documents, or other privileged materials relating to agency communications. Defendants also object to this Interrogatory to the extent it seeks information protected by the deliberative process privilege, attorney-client privilege, law enforcement privilege, a statutory national security privilege, or any other applicable privilege. Additionally, challenges to administrative agency action are ordinarily not subject to discovery outside the administrative record. *Lorion*, 470 U.S. at 743-44. Moreover, this Interrogatory is overbroad, unduly burdensome, and disproportionate to the needs of the case, insofar as it purports to require a response concerning components of the agency or concerning governmental entities outside the agency whose actions are not challenged in the Complaint or Amended Complaint and whose information is not reasonably available to the agency or agency component whose alleged conduct is challenged in the Complaint or Amended Complaint.

Additionally, Defendants object to this Interrogatory as overbroad and disproportional to the needs of the case, particularly in light of the expedited nature of the discovery, to the extent "communication" is meant to cover anything beyond e-mail exchanges.

Further, Defendant objects to this Interrogatory as unreasonably cumulative and duplicative of Common Interrogatories 1 through 5. Defendants otherwise refer Plaintiffs to the documents being produced with these responses for any additional information.

**RESPONSE:** Subject to and without waiving the above objections, HHS has identified OSG, NIAID, and CDC as available sources of information that is potentially responsive to this

**CONFIDENTIAL**

**CONFIDENTIAL**

Interrogatory. In accordance with the Court’s September 6, 2022, Order, HHS responds as follows on behalf of the four HHS identified by the Court: HHS refers to its response to Common Interrogatories 1 through 5 and the accompanying documents. *See generally* Fed. R. Civ. P. 33(d).

**OSG.** Subject to and without waiving the above objections, and based on a reasonable inquiry under the circumstances of abbreviated, expedited discovery, OSG refers to its response to Common Interrogatories 1 through 5 and the accompanying documents. *See generally* Fed. R. Civ. P. 33(d).

**NIAID.** Subject to and without waiving the above objections, and based on a reasonable inquiry under the circumstances of abbreviated, expedited discovery, NIAID refers to its response to Common Interrogatories 1 through 5 and the accompanying documents. *See generally* Fed. R. Civ. P. 33(d).

**CDC.** Subject to and without waiving the above objections, and based on a reasonable inquiry under the circumstances of abbreviated, expedited discovery, CDC refers to its response to Common Interrogatories 1 through 5 and the accompanying documents. *See generally* Fed. R. Civ. P. 33(d).

**Additional Interrogatory No. 4 (CDC No. 7):**

**Identify all “government experts” who are federal officers, officials, agents, employees, or contractors, who have “partnered with” Facebook or any other Social-Media Platform to address Misinformation and/or Content Modulation, including all Communications relating to such partnerships.**

**OBJECTIONS:** Defendants incorporate by reference the above objections. Defendants further object to this Interrogatory as vague because it relies on a characterization of a statement attributed to a third-party, Facebook, as reported in a July 15, 2021 *Reuters.com* article quoted at Compl. ¶ 163, and the statement does not sufficiently specify the individuals at issue or the specific

**CONFIDENTIAL**



**CONFIDENTIAL**

communications referred to. Additionally, Defendants lack information sufficient to establish the meaning of that third party's statement. Defendants further object to this Interrogatory as unduly burdensome and not proportional to the needs of the case. Defendants cannot conduct an exhaustive search to uncover all possible responsive information under the current, abbreviated expedited discovery schedule. Such expedited discovery is especially burdensome given that Defendants' motion to dismiss the Amended Complaint for lack of subject-matter jurisdiction and other deficiencies is forthcoming. Defendant also objects to this Interrogatory as overbroad because it seeks information that is not relevant to Plaintiffs' claims and that does not fall within scope of discovery authorized by the Court. The Court authorized the service of discovery requests concerning "the identity of federal officials who have been and are communicating with social-media platforms about [misinformation and] any censorship or suppression of speech on social media, including the nature and content of those communications." ECF No. 34 at 13. This Interrogatory appears to seek information concerning communications with Social-Media Platforms regardless whether they pertain to content moderation with respect to misinformation. Defendants also object to the Interrogatory to the extent a response requires review of internal, deliberative documents discussing such communications, attorney client documents, or other privileged materials relating to agency communications. Defendants also object to this Interrogatory to the extent it seeks information protected by the deliberative process privilege, attorney-client privilege, law enforcement privilege, a statutory national security privilege, or any other applicable privilege. Additionally, challenges to administrative agency action are ordinarily not subject to discovery outside the administrative record. *Lorion*, 470 U.S. at 743-44. Moreover, this Interrogatory is overbroad, unduly burdensome, and disproportionate to the needs of the case, insofar as it purports to require a response concerning components of the agency or concerning

**CONFIDENTIAL**

**CONFIDENTIAL**

governmental entities outside the agency whose actions are not challenged in the Complaint or Amended Complaint and whose information is not reasonably available to the agency or agency component whose alleged conduct is challenged in the Complaint or Amended Complaint.

Additionally, Defendants object to this Interrogatory as overbroad and disproportional to the needs of the case, particularly in light of the expedited nature of the discovery, to the extent “communication” is meant to cover anything beyond e-mail exchanges.

Further, Defendant objects to this Interrogatory as unreasonably cumulative and duplicative of Common Interrogatories 1 through 5. Defendants otherwise refer Plaintiffs to the documents being produced with these responses for any additional information.

**RESPONSE:** Subject to and without waiving the above objections, and based on a reasonable inquiry under the circumstances of abbreviated, expedited discovery, CDC refers to its response to Common Interrogatories 1 through 5 and the accompanying documents. *See generally* Fed. R. Civ. P. 33(d).

**Additional Interrogatory No. 5 (Dr. Fauci No. 8):**

**Identify all Communications with Mark Zuckerberg from January 1, 2020 to the present, including but not limited to those referenced in Paragraphs 142-145 of the Complaint.**

**OBJECTIONS:** Defendants incorporate by reference the above objections. Defendants further object to this Interrogatory as overbroad because it seeks information that is not relevant to Plaintiffs’ claims and that does not fall within scope of discovery authorized by the Court. The Court authorized the service of discovery requests concerning “the identity of federal officials who have been and are communicating with social-media platforms about [misinformation and] any censorship or suppression of speech on social media, including the nature and content of those communications.” ECF No. 34 at 13. This Interrogatory calls for a response based on all Communications with Mark Zuckerberg, regardless of whether they concern Misinformation.

**CONFIDENTIAL**

**CONFIDENTIAL**

Defendants also understand this Interrogatory to seek only communications between Defendants and third parties outside the government. To the extent that this Interrogatory seeks a response based on internal information referring to such communications, the Interrogatory would be even more disproportional to the needs of the case, as it would require an extensive search of internal records that would not be possible to complete in the expedited period provided for current discovery and would be unnecessary in light of Defendants' agreement to produce the external communications themselves. Defendants also object to the Interrogatory to the extent a response requires review of internal, deliberative documents discussing such communications, attorney client documents, or other privileged materials relating to agency communications. Defendants also object to this Interrogatory to the extent it seeks information protected by the deliberative process privilege, attorney-client privilege, law enforcement privilege, a statutory national security privilege, presidential communications privilege, or any other applicable privilege. Additionally, challenges to administrative agency action are ordinarily not subject to discovery outside the administrative record. *Lorion*, 470 U.S. at 743-44.

Further, Defendants objects to this Interrogatory to the extent it seeks information from Dr. Fauci based on his role as Chief Medical Advisor to the President, on the ground that any discovery on the White House at this stage of the litigation is unduly burdensome and disproportional to the needs of the case. Plaintiffs have not exhausted all other avenues of discovery before seeking discovery on the White House. *See, e.g.,* Order, *Centro Presente*, No. 1:18-cv-10340 (D. Mass. May 15, 2019); *Karnoski v. Trump*, 926 F.3d 1180, 1207 (9th Cir. 2019); *Cheney*, 542 U.S. at 390. Additionally, discovery propounded on White House officials would create an undue burden, distract them from their critical executive responsibilities, and violate the separation of powers. *See Cheney*, 542 U.S. at 385. That burden is especially undue at this stage of the litigation given

**CONFIDENTIAL**

**CONFIDENTIAL**

that Defendants' motion to dismiss the Amended Complaint for lack of subject-matter jurisdiction and other deficiencies is forthcoming. Additionally, Defendants object to this Interrogatory to the extent it a response requires review of information protected by the presidential communications privilege or other executive privileges. *See Nixon*, 418 U.S. at 708. Because Plaintiffs are not entitled to such documents, the Interrogatory imposes a burden on Defendants to locate documents and review them that is disproportional to the minimal benefit (if any) that Plaintiffs might derive from the possibility of an Interrogatory response based on responsive non-privileged documents. *See Cheney*, 542 U.S. at 389. Defendants, however, aver that Dr. Fauci does not have a White House e-mail address and have provided responses, subject to any other objections, in his capacity as Director of NIAID.

Additionally, Defendants object to this Interrogatory as overbroad and disproportional to the needs of the case, particularly in light of the expedited nature of the discovery, to the extent "communication" is meant to cover anything beyond e-mail exchanges.

Further, Defendant objects to this Interrogatory as unreasonably cumulative and duplicative of Common Interrogatories 1 through 5.

**RESPONSE:** Subject to and without waiving the above objections, and based on a reasonable inquiry under the circumstances of abbreviated, expedited discovery, NIAID responds on behalf of Dr. Fauci, and refers to NIAID's responses to Common Interrogatories 1 through 5 and the accompanying documents. *See generally* Fed. R. Civ. P. 33(d).

Further, in accordance with the Court's September 6, 2022 Order, subject to and without waiving any of the foregoing objections, and based on a reasonable inquiry under the circumstances of abbreviated, expedited discovery, including consultation with Dr. Fauci and

**CONFIDENTIAL**

**CONFIDENTIAL**

review of Dr. Fauci and NIAID staff e-mail records, NIAID responds on behalf of Dr. Fauci in his role as Director of NIAID as follows: NIAID has identified the following communications:

- On February 27, 2020, Dr. Fauci received an email from Mark Zuckerberg, with no subject line, a copy of which was produced at MOLA\_DEFSPROD\_00004560.
- On February 27, 2020, Dr. Fauci emailed Mark Zuckerberg, with the subject line “RE:” a copy of which was produced at MOLA\_DEFSPROD\_00004564.
- On March 15, 2020, Dr. Fauci received an email from Mark Zuckerberg, with the subject line “Thanks and ideas”, a copy of which was produced at MOLA\_DEFSPROD\_00015091.
- On March 16, 2020, Dr. Fauci attempted to call Mark Zuckerberg but received his voicemail.
- On March 16, 2020, Dr. Fauci emailed Mark Zuckerberg, with the subject line “RE: Thanks and ideas”, a copy of which was produced at MOLA\_DEFSPROD\_00015095.
- On March 16, 2020, Dr. Fauci received an email from Mark Zuckerberg, with the subject line “RE: Thanks and ideas”, a copy of which was produced at MOLA\_DEFSPROD\_00015089.
- On March 19, 2020, Dr. Fauci participated in a Facebook Live event with Mark Zuckerberg that was broadcast on Facebook beginning at approximately 7:00 pm Eastern Time to discuss COVID-19. A recording of this event is available at <https://www.facebook.com/zuck/videos/10111683294466031>.
- On April 8, 2020, Dr. Fauci received an email from Mark Zuckerberg, without a subject line, a copy of which was produced at MOLA\_DEFSPROD\_00004559.

**CONFIDENTIAL**

**CONFIDENTIAL**

- On April 9, 2020, Dr. Fauci emailed Mark Zuckerberg, with the subject line “RE:”, a copy of which was produced at MOLA\_DEFSPROD\_00004563.
- As indicated by MOLA\_DEFSPROD\_00006375, it appears that Dr. Fauci and Mark Zuckerberg may have spoken via telephone on July 14, 2020, about the upcoming Facebook Live event. However, Dr. Fauci has no specific recollection of that call.
- On July 16, 2020, Dr. Fauci participated in a Facebook Live event with Mark Zuckerberg that was broadcast on Facebook beginning at approximately 5:00pm Eastern Time to discuss COVID-19. The event took place using Zoom. A recording of this event is available at <https://www.facebook.com/zuck/videos/10112108870243761/>. Immediately prior to the Facebook Live event, Dr. Fauci and Mark Zuckerberg may have briefly met in a virtual green room.
- On November 29, 2020, at approximately 6:30pm Eastern Time, Dr. Fauci and Mark Zuckerberg spoke via telephone about the upcoming Facebook Live event.
- On November 30, 2020, Dr. Fauci participated in a Facebook Live event with Mark Zuckerberg that was broadcast on Facebook beginning at approximately 3:00pm Eastern Time to discuss COVID-19 and progress towards a COVID-19 vaccine. The event took place using Zoom. A recording of this event is available at <https://www.facebook.com/zuck/videos/10112595016437891>. Immediately prior to the Facebook Live event, Dr. Fauci and Mark Zuckerberg may have briefly met in a virtual green room.

**Additional Interrogatory No. 6 (Dr. Fauci No. 9):**

**Identify all Communications with any Social-Media Platform that relate to the Great Barrington Declaration, the authors of the Great Barrington Declaration, the original signers of the Great Barrington Declaration, Dr. Jay Bhattacharya, Dr. Martin Kulldorff, Dr. Aaron Kheriaty, Dr. Sunetra Gupta, Dr. Scott Atlas, Alex Berenson, Dr. Peter Daszak,**

**CONFIDENTIAL**

**CONFIDENTIAL**

**Dr. Shi Zhengli, the Wuhan Institute of Virology, EcoHealth Alliance, and/or any member of the so-called “Disinformation Dozen.”**

**OBJECTIONS:** Defendants incorporate by reference the above objections. Defendants further object to this Interrogatory as vague because it does not define what the “Great Barrington Declaration” is or who the “Disinformation Dozen” are. Defendants further object to this Interrogatory as unduly burdensome and not proportional to the needs of the case. Defendants cannot conduct an exhaustive search to uncover all possible responsive information under the current, abbreviated expedited discovery schedule. Such expedited discovery is especially burdensome given that Defendants’ motion to dismiss the Amended Complaint for lack of subject-matter jurisdiction and other deficiencies is forthcoming. Defendants also object to this Interrogatory as overbroad because it requests information that does not fall within the scope of discovery authorized by the Court. The Court authorized the service of discovery requests concerning “the identity of federal officials who have been and are communicating with social-media platforms about [misinformation and] any censorship or suppression of speech on social media, including the nature and content of those communications.” ECF No. 34 at 13. This Interrogatory seeks information concerning, *inter alia*, the Great Barrington Declaration, its authors, its original signers, and any member of the “Disinformation Dozen,” regardless whether the Communications sought concern Misinformation. Defendants also understand this Interrogatory to seek only a response based on communications between Defendants and third parties outside the Government. Defendants also object to the Interrogatory to the extent a response requires review of internal, deliberative documents discussing such communications, attorney client documents, or other privileged materials relating to agency communications. Defendants also object to this Interrogatory to the extent it seeks information protected by the deliberative process privilege, attorney-client privilege, law enforcement privilege, a statutory national security

**CONFIDENTIAL**

**CONFIDENTIAL**

privilege, presidential communications privilege, or any other applicable privilege. Additionally, challenges to administrative agency action are ordinarily not subject to discovery outside the administrative record. *Lorion*, 470 U.S. at 743-44.

Further, Defendants object to this Interrogatory to the extent it seeks information from Dr. Fauci based on his role as Chief Medical Advisor to the President, on the ground that any discovery on the White House at this stage of the litigation is unduly burdensome and disproportional to the needs of the case. Plaintiffs have not exhausted all other avenues of discovery before seeking discovery on the White House. *See, e.g.*, Order, *Centro Presente*, No. 1:18-cv-10340 (D. Mass. May 15, 2019); *Karnoski v. Trump*, 926 F.3d 1180, 1207 (9th Cir. 2019); *Cheney*, 542 U.S. at 390. Additionally, discovery propounded on White House officials would create an undue burden, distract them from their critical executive responsibilities, and violate the separation of powers. *See Cheney*, 542 U.S. at 385. That burden is especially undue at this stage of the litigation given that Defendants' motion to dismiss the Amended Complaint for lack of subject-matter jurisdiction and other deficiencies is forthcoming. Additionally, Defendants object to this Interrogatory to the extent it a response requires review of information protected by the presidential communications privilege or other executive privileges. *See Nixon*, 418 U.S. at 708. Because Plaintiffs are not entitled to such documents, the Interrogatory imposes a burden on Defendants to locate documents and review them that is disproportional to the minimal benefit (if any) that Plaintiffs might derive from the possibility of an Interrogatory response based on responsive non-privileged documents. *See Cheney*, 542 U.S. at 389.

Additionally, Defendants object to this Interrogatory as overbroad and disproportional to the needs of the case, particularly in light of the expedited nature of the discovery, to the extent "communication" is meant to cover anything beyond e-mail exchanges.

**CONFIDENTIAL**



**CONFIDENTIAL**

Further, Defendant objects to this Interrogatory as unreasonably cumulative and duplicative of Common Interrogatories 1 through 5.

**RESPONSE:** Subject to and without waiving the above objections, and based on a reasonable inquiry under the circumstances of abbreviated, expedited discovery, NIAID responds on behalf of Dr. Fauci, and refers to NIAID's responses to Common Interrogatories 1 through 5 and the accompanying documents. *See generally* Fed. R. Civ. P. 33(d).

Further, in accordance with the Court's September 6, 2022 Order, subject to and without waiving any of the foregoing objections, and based on a reasonable inquiry under the circumstances of abbreviated, expedited discovery, including consultation with Dr. Fauci and review of Dr. Fauci and NIAID staff e-mail records, NIAID responds on behalf of Dr. Fauci in his role as Director of NIAID as follows: NIAID has not identified any communications, written or oral, between Dr. Fauci and Social-Media Platforms relating to the Great Barrington Declaration, the authors of the Great Barrington Declaration, the original signers of the Great Barrington Declaration, Dr. Jay Bhattacharya, Dr. Martin Kulldorff, Dr. Aaron Kheriaty, Dr. Sunetra Gupta, Dr. Scott Atlas, Alex Berenson, Dr. Peter Daszak, Dr. Shi Zhengli, the Wuhan Institute of Virology, EcoHealth Alliance, and/or any member of the so-called "Disinformation Dozen." In general, Dr. Fauci has participated in media appearances and communications with or on Social-Media Platforms to publicize health information and provide COVID-19 and vaccine education. Dr. Fauci's media appearances on Social-Media Platforms are not responsive to this request. It is possible that the topics or individuals above were mentioned in public media appearances on Social-Media Platforms in which Dr. Fauci participated but NIAID, including in consultation with Dr. Fauci, have not identified any such examples involving Dr. Fauci's communications with Social-Media Platforms.

**CONFIDENTIAL**

**CONFIDENTIAL**

**Additional Interrogatory No. 7 (Dr. Fauci No. 10):**

**Identify all Communications between any member of the White House Communications Team and any Social-Media Platform that refer or relate to Misinformation and/or Content Modulation.**

**OBJECTIONS:** Defendants incorporate by reference the above objections. Defendants also object to this Interrogatory to the extent it seeks information protected by the deliberative process privilege, attorney-client privilege, law enforcement privilege, a statutory national security privilege, presidential communications privilege, or any other applicable privilege. Defendants further object to this Interrogatory to the extent it seeks information from Dr. Fauci based on his role as Chief Medical Advisor to the President, on the ground that any discovery on the White House at this stage of the litigation is unduly burdensome and disproportional to the needs of the case. Plaintiffs have not exhausted all other avenues of discovery before seeking discovery on the White House. See, e.g., Order, *Centro Presente*, No. 1:18-cv-10340 (D. Mass. May 15, 2019); *Karnoski v. Trump*, 926 F.3d 1180, 1207 (9th Cir. 2019); *Cheney*, 542 U.S. at 390. Additionally, discovery propounded on White House officials would create an undue burden, distract them from their critical executive responsibilities, and violate the separation of powers. See *Cheney*, 542 U.S. at 385. That burden is especially undue at this stage of the litigation given that Defendants' motion to dismiss the Amended Complaint for lack of subject-matter jurisdiction and other deficiencies is forthcoming. Additionally, Defendants object to this Interrogatory to the extent it seeks information protected by the presidential communications privilege or other executive privileges. See *Nixon*, 418 U.S. at 708. Defendants, however, aver that Dr. Fauci does not have a White House e-mail address and have provided responses, subject to any other objections, in his capacity as Director of NIAID.

**CONFIDENTIAL**

**CONFIDENTIAL**

Additionally, Defendants object to this Interrogatory as overbroad and disproportional to the needs of the case, particularly in light of the expedited nature of the discovery, to the extent “communication” is meant to cover anything beyond e-mail exchanges.

Further, Defendant objects to this Interrogatory as unreasonably cumulative and duplicative of Common Interrogatories 1 through 5.

**RESPONSE:** Subject to and without waiving the above objections, and based on a reasonable inquiry under the circumstances of abbreviated, expedited discovery, NIAID responds on behalf of Dr. Fauci, and refers to NIAID’s responses to Common Interrogatories 1 through 5 and the accompanying documents. *See generally* Fed. R. Civ. P. 33(d).

**Additional Interrogatory No. 8 (DHS No. 6):**

**Define what is an “Analytic Exchange” with Twitter or any other Social-Media Platform, and identify any existing “Analytic Exchanges,” including all participant(s) in such Analytic Exchange(s).**

**OBJECTIONS:** Defendants incorporate by reference the above objections. Defendants object to this Interrogatory as overbroad and disproportional to the needs of the case because it calls for information that is not relevant to Plaintiffs’ claims and that do not fall within the scope of discovery authorized by the Court. The Court authorized the service of discovery requests concerning “the identity of federal officials who have been and are communicating with social-media platforms about [misinformation and] any censorship or suppression of speech on social media, including the nature and content of those communications.” ECF No. 34 at 13. This Interrogatory asks Defendants to define “Analytic Exchange(s),” and identify any such “Analytic Exchange(s),” regardless whether those communications pertain to Misinformation. Defendants also object to the Interrogatory to the extent a response requires review of internal, deliberative documents discussing such communications, attorney client documents, or other privileged materials relating to agency

**CONFIDENTIAL**

**CONFIDENTIAL**

communications. Defendants also object to this Interrogatory to the extent it seeks information protected by the deliberative process privilege, attorney-client privilege, law enforcement privilege, a statutory national security privilege, or any other applicable privilege. Additionally, challenges to administrative agency action are ordinarily not subject to discovery outside the administrative record. *Lorion*, 470 U.S. at 743-44.

**RESPONSE:** Subject to and without waiving the above objections, Defendant DHS responds as follows: DHS has not defined the term ‘Analytic Exchange’ as a matter of departmental policy. For purposes of this response, DHS defines the term as an arrangement between DHS and external entities under which the participants exchange information and analysis regarding threats or vulnerabilities relating to homeland security on a periodic basis.

The DHS Office of Intelligence and Analysis participates in a number of Analytic Exchanges, including one where Misinformation is a topic of interest. Specifically, the Office of Intelligence and Analysis, on behalf of the Office of the Director of National Intelligence, sponsors the Public-Private Analytic Exchange Program (“AEP”). The AEP facilitates collaborative partnerships between members of the private sector and teams of experienced U.S. government analysts to form a number of subcommittees. This annual program provides U.S. government analysts and private sector partners with a better understanding of select national security and homeland security issues.

There are approximately 100 participants in the AEP. Each year, teams of analysts drawn from the AEP participants work virtually over six months to develop unclassified intelligence products made available to the public. Among the topics to be addressed by the AEP this year are “Countering Foreign Malign Social Network Manipulation in the Homeland,” “Addressing Risks From Non-State Actors’ Use of Commercially Available Technologies,” and “Phase II: Increasing

**CONFIDENTIAL**

**CONFIDENTIAL**

Threats of Deepfake Identities.” All three of these topics are expected to address Misinformation in some form. Finished products for all of the AEP 2022 topics will be presented at the AEP Concluding Summit scheduled for August 30–31 and will be made available on the DHS website: <https://www.dhs.gov/aep-deliverables>.

**Additional Interrogatory No. 9 (DHS No. 7):**

**Identify all participants and topics of discussion in the “series of monthly meetings between the government and tech companies” prior to the 2020 election, as discussed in Paragraphs 182-184 of the Complaint.**

**OBJECTIONS:** Defendants incorporate by reference the above objections. Defendants further object to this Interrogatory as vague because it relies on a characterization of statements made by third-party companies, rather than any Defendant, as reported in an August 12, 2020 *NBC News.com* article cited at Compl. ¶ 180, and the statements do not provide sufficient details of the meetings to which the Interrogatory refers. Defendants also object to this Interrogatory as unduly burdensome and not proportional to the needs of the case. This Interrogatory calls for information about meetings that occurred before the current President took office. Defendants also object to this Interrogatory as overbroad and disproportional to the needs of the case because it calls for information that is not relevant to Plaintiffs’ claims and that do not fall within scope of discovery authorized by the Court. The Court authorized the service of discovery requests concerning “the identity of federal officials who have been and are communicating with social-media platforms about [misinformation and] any censorship or suppression of speech on social media, including the nature and content of those communications.” ECF No. 34 at 13. Defendants also object because the undefined term “tech companies” as used in this Interrogatory is vague and ambiguous. This Interrogatory appears to call for information relating to certain meetings with technology companies that occurred prior to the 2020 election, regardless whether those meetings were with Social-Media Platforms and pertained to Misinformation. Defendants also object to the

**CONFIDENTIAL**

**CONFIDENTIAL**

Interrogatory to the extent a response requires review of internal, deliberative documents discussing such communications, attorney client documents, or other privileged materials relating to agency communications. Defendants also object to this Interrogatory to the extent it seeks information protected by the deliberative process privilege, attorney-client privilege, law enforcement privilege, a statutory national security privilege, or any other applicable privilege. Additionally, challenges to administrative agency action are ordinarily not subject to discovery outside the administrative record. *Lorion*, 470 U.S. at 743-44.

**RESPONSE:** Subject to and without waiving the above objections, Defendant DHS responds as follows: The “series of monthly meetings between the government and tech companies” relates to a recurring meeting with federal government officials and the private industry, and the participants and topics of discussion have evolved over time. Government participants have included various representatives from CISA, DHS’s Office of Intelligence and Analysis, the FBI’s Foreign Influence Task Force, the Justice Department’s National Security Division, and the Office of the Director of National Intelligence. Industry participants have included representatives from Google, Facebook, Twitter, Reddit, Microsoft, Verizon Media, Pinterest, LinkedIn and the Wikimedia Foundation. The topics discussed include, but are not limited to: information sharing around elections risk, briefs from industry, threat updates, and highlights and upcoming watch outs. DHS refers to its responses to Common Interrogatories 1 through 5 and the accompanying documents, *see generally* Fed. R. Civ. P. 33(d), for information about individual meeting invitations and agendas.

**Additional Interrogatory No. 10 (DHS No. 8):**

**Identify all “private firms” that DHS has “partnered” with, or planned, intended, or discussed “partnering” with, to “monitor” online content, as discussed in Paragraph 202 of**

**CONFIDENTIAL**

**CONFIDENTIAL**

**the Complaint, including the nature of the “partnership” and the nature of any “outsourcing [of] information gathering to outside firms.”**

**OBJECTIONS:** Defendants incorporate by reference the above objections. Defendants further object to this Interrogatory because it seeks information that is not relevant to Plaintiffs’ claims and does not fall within the scope of discovery authorized by the Court. The Court authorized the service of discovery requests concerning “the identity of federal officials who have been and are communicating with social-media platforms about [misinformation and] any censorship or suppression of speech on social media, including the nature and content of those communications.” ECF No. 34 at 13. This Interrogatory would require identification of outside “private firms” rather than identification of federal officials; and it would require describing the nature of any “planned, intended, or discussed ‘partnerships’” rather than the nature and content of communications with social-media platforms. Defendants also object to this Interrogatory to the extent it seeks information protected by the deliberative process privilege, attorney-client privilege, law enforcement privilege, a statutory national security privilege, or any other applicable privilege. Additionally, challenges to administrative agency action are ordinarily not subject to discovery outside the administrative record. *Lorion*, 470 U.S. at 743-44.

Defendants also object to the Interrogatory to the extent a response requires review of internal, deliberative documents discussing such communications, attorney client documents, or other privileged materials relating to agency communications. Defendants also object to this Interrogatory as “vague” because it does not define what constitutes a “private firm,” or what is meant by “partner,” “monitor,” or “outsourcing” information gathering. Defendants also object to this Interrogatory as overbroad because it calls for identification of every “private firm” that DHS may have “planned, intended, or discussed” partnering with.

**RESPONSE:** Subject to and without waiving the above objections, Defendant DHS

**CONFIDENTIAL**

**CONFIDENTIAL**

responds as follows: As DHS responded in the news article Plaintiffs cited to in support of the allegations in the Complaint to which this Interrogatory refers, DHS “is not partnering with private firms to surveil suspected domestic terrorists online.” <https://www.cnn.com/2021/05/03/politics/dhs-partner-private-firms-surveil-suspected-domestic-terrorists/index.html>. DHS does not partner with “private firms” to “to evade legal, constitutional, and ethical problems with DHS’s direct surveillance of online speech.”

**Additional Interrogatory No. 11 (DHS No. 9):**

**Identify all “the tech companies” with which DHS is “working together” to “prevent harm from occurring,” as Secretary Mayorkas stated on August 2, 2021, as discussed in Paragraph 207-208 of the Complaint, including the nature of the work and all Communication(s) relating to such work.**

**OBJECTIONS:** Defendants incorporate by reference the above objections. Defendants also object because the undefined term “tech companies” as used in this Interrogatory is vague and ambiguous. Even assuming that the term “tech companies” is the same as the term “Social-Media Platform[s]” as defined by Plaintiffs, Defendants further object to this Interrogatory as unduly burdensome and not proportional to the needs of the case. Defendants cannot conduct an exhaustive search to uncover all possible responsive information under the current, abbreviated expedited discovery schedule. Such expedited discovery is especially burdensome given that Defendants’ motion to dismiss the Amended Complaint for lack of subject-matter jurisdiction and other deficiencies is forthcoming. Defendants also object to this Interrogatory as overbroad because it seeks information that is not relevant to Plaintiffs’ claims and that do not fall within scope of discovery authorized by the Court. The Court authorized the service of discovery requests concerning “the identity of federal officials who have been and are communicating with social-media platforms about [misinformation and] any censorship or suppression of speech on social media, including the nature and content of those communications.” ECF No. 34 at 13. This Interrogatory appears to seek

**CONFIDENTIAL**



**CONFIDENTIAL**

information relating to efforts to work with private “tech” companies to “prevent harm from occurring,” regardless of whether those efforts pertained to Misinformation. Defendants also object to the Interrogatory to the extent a response requires review of internal, deliberative documents discussing such communications, attorney client documents, or other privileged materials relating to agency communications. Defendants also object to this Interrogatory to the extent it seeks information protected by the deliberative process privilege, attorney-client privilege, law enforcement privilege, a statutory national security privilege, or any other applicable privilege. Additionally, challenges to administrative agency action are ordinarily not subject to discovery outside the administrative record. *Lorion*, 470 U.S. at 743-44.

Additionally, Defendants object to this Interrogatory as overbroad and disproportional to the needs of the case, particularly in light of the expedited nature of the discovery, to the extent “communication” is meant to cover anything beyond e-mail exchanges.

Further, Defendant objects to this Interrogatory as unreasonably cumulative and duplicative of Common Interrogatories 1 through 5. Defendants otherwise refer Plaintiffs to the documents being produced with these responses for any additional information.

**RESPONSE:** Subject to and without waiving the above objections, DHS refers to its response to Common Interrogatories 1 through 5 and the accompanying documents, *see generally* Fed. R. Civ. P. 33(d), and further responds as follows: Consistent with the Department’s mission to protect the homeland, DHS responds to Misinformation that poses a threat to the homeland. It identifies Misinformation that poses a threat to the homeland through publicly available sources, research conducted by academic and other institutions, and information shared by other federal agencies and partners. DHS then shares factual information related to its mission and about which it has expertise to potentially impacted people and organizations.

**CONFIDENTIAL**

**CONFIDENTIAL**

**Additional Interrogatory No. 12 (DHS No. 13):**

**Identify every federal agency, group, sub-group, department, component, division, sub-division, officer, official, employee, agent, or other person or entity within the federal government, both within and without DHS, that communicates or has communicated with any Social-Media Platform regarding Misinformation and/or Content Modulation, including but not limited to any person or entity whose activity is or was to be subject to oversight by the Disinformation Governance Board, including the nature of their coordination with the Social-Media Platform(s).**

**OBJECTIONS:** Defendants incorporate by reference the above objections. Defendants further object to this Interrogatory as overbroad and unduly burdensome to the extent it seeks identification of every “person or entity within the federal government,” including those “without DHS,” that “communicates or has communicated with any Social-Media Platform.” This Interrogatory appears to call on Defendants to exceed the information reasonably available to them and thus goes beyond the scope of Rules 26 and 33. Even if such an Interrogatory were proper as to the conduct of the named Defendants, it would still be overbroad and disproportional to the needs of the case to the extent it seeks information about any agency that is not a Defendant in this action. Defendants further object to this Interrogatory as overbroad and cumulative to the extent it seeks information requested in earlier interrogatories, in particular Interrogatory 1, that also seek identification of individuals who have communicated with or are communicating with a social-media platform regarding Misinformation. Defendants additionally object to this Interrogatory as vague because it does not define what constitutes “coordination.” Defendants also object to this Interrogatory as overbroad and unduly burdensome to the extent it seeks a description of “the nature of . . . coordination” between any and all “person[s] or entit[ies] within the federal government” and a “Social-Media Platform.” Defendants also object to this Interrogatory to the extent it seeks information protected by the deliberative process privilege, attorney-client privilege, law enforcement privilege, a statutory national security privilege, or any other applicable

**CONFIDENTIAL**

**CONFIDENTIAL**

privilege. Additionally, challenges to administrative agency action are ordinarily not subject to discovery outside the administrative record. *Lorion*, 470 U.S. at 743-44. Moreover, this Interrogatory is overbroad, unduly burdensome, and disproportionate to the needs of the case, insofar as it purports to require a response concerning components of the agency or concerning governmental entities outside the agency whose actions are not challenged in the Complaint or Amended Complaint and whose information is not reasonably available to the agency or agency component whose alleged conduct is challenged in the Complaint or Amended Complaint.

Additionally, Defendants object to this Interrogatory as overbroad and disproportional to the needs of the case, particularly in light of the expedited nature of the discovery, to the extent “communication” is meant to cover anything beyond e-mail exchanges.

Further, Defendant objects to this Interrogatory as unreasonably cumulative and duplicative of Common Interrogatories 1 through 5. Defendants otherwise refer Plaintiffs to the documents being produced with these responses for any additional information.

**RESPONSE:** Subject to and without waiving any of the foregoing objections, DHS responds as follows: DHS components lead on operational efforts to counter Misinformation in their relevant mission spaces. Within DHS HQ, personnel from within DHS’s Office of Intelligence & Analysis, Office of Strategy, Policy, and Plans, Office of Public Affairs, and Disinformation Governance Board have communicated with Social-Media Platforms regarding Misinformation.

**Additional Interrogatory No. 13 (DHS No. 14):**

**Identify every federal agency, group, sub-group, department, component, division, sub-division, officer, official, employee, agent, or other person or entity within DHS that is involved in “counter-disinformation efforts” and, as part of those efforts, communicates or has communicated with any Social-Media Platform, including the nature of such “counter-disinformation efforts.”**

**CONFIDENTIAL**

**CONFIDENTIAL**

**OBJECTIONS:** Defendants incorporate by reference the above objections. Defendants also object because the undefined term “counter-disinformation efforts” is vague, and ambiguous. Defendants further object to this Interrogatory because it seeks information that is not relevant to Plaintiffs’ claims and does not fall within the scope of discovery authorized by the Court. The Court authorized the service of discovery requests concerning “the identity of federal officials who have been and are communicating with social-media platforms about [misinformation and] any censorship or suppression of speech on social media, including the nature and content of those communications.” ECF No. 34 at 13. This Interrogatory, however, also asks Defendants to describe “the nature of . . . ‘counter-disinformation efforts,’” independent of any communications with social media platforms and thus goes beyond the scope of discovery authorized by the Court. Defendants also object to this Interrogatory to the extent it seeks information protected by the deliberative process privilege, attorney-client privilege, law enforcement privilege, a statutory national security privilege, or any other applicable privilege. Additionally, challenges to administrative agency action are ordinarily not subject to discovery outside the administrative record. *Lorion*, 470 U.S. at 743-44. Moreover, this Interrogatory is overbroad, unduly burdensome, and disproportionate to the needs of the case, insofar as it purports to require a response concerning components of the agency or concerning governmental entities outside the agency whose actions are not challenged in the Complaint or Amended Complaint and whose information is not reasonably available to the agency or agency component whose alleged conduct is challenged in the Complaint or Amended Complaint.

Additionally, Defendants object to this Interrogatory as overbroad and disproportional to the needs of the case, particularly in light of the expedited nature of the discovery, to the extent “communication” (“communicates or has communicated”) is meant to cover anything beyond e-

**CONFIDENTIAL**

**CONFIDENTIAL**

mail exchanges.

Further, Defendant objects to this Interrogatory as unreasonably cumulative and duplicative of Common Interrogatories 1 through 5. Defendants otherwise refer Plaintiffs to the documents being produced with these responses for any additional information.

**RESPONSE:** Subject to and without waiving the above objections, DHS responds as follows: DHS components lead on operational efforts to counter Misinformation in their relevant mission spaces. Within DHS HQ, personnel from within DHS’s Office of Intelligence & Analysis, Office of Strategy, Policy, and Plans, and Disinformation Governance Board have communicated with Social-Media Platforms regarding Misinformation. The nature of DHS’s work is that it identifies Misinformation that threatens the homeland through publicly available sources, research conducted by academic and other institutions, and information shared by other federal agencies and partners. DHS then shares factual information related to its mission to potentially impacted people and organizations.

**Additional Interrogatory No. 14 (Jankowicz No. 9):**

**Identify the nature, purpose, participants, topics to be discussed, and topics actually discussed at the meeting between DHS personnel and Twitter executives Nick Pickles and Yoel Roth scheduled on or around April 28, 2022.**

**OBJECTIONS:** Defendants incorporate by reference the above objections. Defendants further object to this Interrogatory as unduly burdensome and not proportional to the needs of the case. Defendants cannot conduct an exhaustive search to uncover all possible responsive information under the current, abbreviated expedited discovery schedule. Such expedited discovery is especially burdensome given that Defendants’ motion to dismiss the Amended Complaint for lack of subject-matter jurisdiction and other deficiencies is forthcoming. Defendants also objects to this Interrogatory as overbroad because it information that is not relevant to Plaintiffs’ claims and that do not fall within

**CONFIDENTIAL**

**CONFIDENTIAL**

scope of discovery authorized by the Court. The Court authorized the service of discovery requests concerning “the identity of federal officials who have been and are communicating with social-media platforms about [misinformation and] any censorship or suppression of speech on social media, including the nature and content of those communications.” ECF No. 34 at 13. This Interrogatory appears to call for information relating to a specific meeting with two identified employees of Social-Media Platforms, or “any similar meeting with [any other] personnel associated with any Social-Media Platform,” regardless whether those communications pertain to Misinformation. Defendants also object to the Interrogatory to the extent a response requires review of internal, deliberative documents discussing such communications, attorney client documents, or other privileged materials relating to agency communications. Defendants also object to this Interrogatory to the extent it seeks information protected by the deliberative process privilege, attorney-client privilege, law enforcement privilege, a statutory national security privilege, or any other applicable privilege. Additionally, challenges to administrative agency action are ordinarily not subject to discovery outside the administrative record. *Lorion*, 470 U.S. at 743-44.

**RESPONSE:** Subject to and without waiving the above objections, Defendant DHS responds on behalf of Ms. Jankowicz, and responds as follows: The April 28, 2022 meeting between DHS personnel and Twitter executives Nick Pickles and Yoel Roth did not occur.

**Additional Interrogatory No. 15 (Ms. Easterly No. 8):**

**Identify every working group, “analytic exchange,” task force, joint government-private enterprise, or similar formal or informal arrangement that involves federal official(s) communicating with any Social-Media Platform(s) about Content Modulation and/or Misinformation, including all participants in such groups.**

**OBJECTIONS:** Defendants incorporate by reference the above objections. Defendants further object to this Interrogatory as vague because it does not define key terms, including “working group” and “arrangement.” Defendants further object to this Interrogatory as unduly

**CONFIDENTIAL**

**CONFIDENTIAL**

burdensome and not proportional to the needs of the case. This Interrogatory calls for a response based on any and all specified communications (“arrangement . . . communicating”) from any Defendant or any employee or subordinate of any Defendant. Defendants cannot conduct an exhaustive search to uncover all possible responsive information under the current, abbreviated expedited discovery schedule. Location of information about every “federal official” communicating with “any Social-Media Platform[]” would require a search that is not feasible under the current, abbreviated expedited discovery schedule. Defendants also object to the Interrogatory to the extent a response requires review of internal, deliberative documents discussing such communications, attorney client documents, or other privileged materials relating to agency communications. Defendants also object to this Interrogatory to the extent it seeks information protected by the deliberative process privilege, attorney-client privilege, law enforcement privilege, a statutory national security privilege, or any other applicable privilege. Additionally, challenges to administrative agency action are ordinarily not subject to discovery outside the administrative record. *Lorion*, 470 U.S. at 743-44. Moreover, this Interrogatory is overbroad, unduly burdensome, and disproportionate to the needs of the case, insofar as it purports to require a response concerning components of the agency or concerning governmental entities outside the agency (“federal official(s)”) whose actions are not challenged in the Complaint or Amended Complaint and whose information is not reasonably available to the agency or agency component whose alleged conduct is challenged in the Complaint or Amended Complaint.

Additionally, Defendants object to this Interrogatory as overbroad and disproportional to the needs of the case, particularly in light of the expedited nature of the discovery, to the extent “communicating” is meant to cover anything beyond e-mail exchanges.

Further, Defendant objects to this Interrogatory as unreasonably cumulative and duplicative

**CONFIDENTIAL**

**CONFIDENTIAL**

of Common Interrogatories 1 through 5. Defendants otherwise refer Plaintiffs to the documents being produced with these responses for any additional information.

**RESPONSE:** Subject to and without waiving the above objections, Defendant CISA responds on behalf of Ms. Easterly, and refers to the response to Common Interrogatories 1 through 5 and the accompanying documents, *see generally* Fed. R. Civ. P. 33(d), and further responds as follows:

Working groups, “analytic exchanges,” task forces, joint government-private enterprises, or similar formal or informal arrangements that involve CISA officials communicating with Social-Media Platforms about Misinformation, include, but are not limited to:

- CISA’s Mis-, Dis-, and Malinformation (MDM) team, formerly known as the CFITF. The CFITF was established in May 2018 in CISA’s predecessor agency. The CFITF was charged with helping the American people understand the risks from MDM and how citizens can play a role in reducing the impact of MDM on their organizations and communities. In 2021, the CFITF officially transitioned to CISA’s MDM team, and the mission evolved to reflect the changing information environment. The MDM team continues to work in close coordination with interagency and private sector partners, social media companies, academia, and international partners on a variety of projects to build resilience against malicious information activities.
- A recurring engagement between USG – Industry, as described in response to Common Interrogatory No. 4.
- CISA CSAC, including the Protecting Critical Infrastructure from Misinformation and Disinformation Subcommittee, as described in response to [Interrogatory No. 4]. Additional information about the CSAC is available on CISA’s website,

**CONFIDENTIAL**



**CONFIDENTIAL**

<https://www.cisa.gov/cisa-cybersecurity-advisory-committee>.

- The EIS-GCC and EI-SCC Joint MDM Working Group, as described in response to Common Interrogatory No. 4.

**Additional Interrogatory No. 16 (Ms. Easterly No. 10):**

**Identify every instance in which CISA’s “MDM team” has “serve[d] as a switchboard for routing disinformation concerns to appropriate social media platforms,” as stated in Your April 12, 2022 bulletin, including all Communication(s) related to such instance.**

**OBJECTIONS:** Defendants incorporate by reference the above objections. Defendants further object to this Interrogatory as unduly burdensome and not proportional to the needs of the case. This Interrogatory calls Defendant to identify “every instance” in which CISA’s “MDM team” “rout[ed] disinformation concerns.” Defendants cannot conduct an exhaustive search to uncover all possible responsive information under the current, abbreviated expedited discovery schedule. Such expedited discovery is especially burdensome given that Defendants’ motion to dismiss the Amended Complaint for lack of subject-matter jurisdiction and other deficiencies is forthcoming. Defendants also object to the Interrogatory to the extent a response requires review of internal, deliberative documents discussing such communications, attorney client documents, or other privileged materials relating to agency communications. Defendants also object to this Interrogatory to the extent it seeks information protected by the deliberative process privilege, attorney-client privilege, law enforcement privilege, a statutory national security privilege, or any other applicable privilege. Additionally, challenges to administrative agency action are ordinarily not subject to discovery outside the administrative record. *Lorion*, 470 U.S. at 743-44.

Additionally, Defendants object to this Interrogatory as overbroad and disproportional to the needs of the case, particularly in light of the expedited nature of the discovery, to the extent “communication” is meant to cover anything beyond e-mail exchanges.

**CONFIDENTIAL**

**CONFIDENTIAL**

Further, Defendant objects to this Interrogatory as unreasonably cumulative and duplicative of Common Interrogatories 1 through 5.

**RESPONSE:** Subject to and without waiving the above objections, Defendant CISA responds on behalf of Ms. Easterly, and refers to the response to Common Interrogatories 1 through 5 and the accompanying documents, *see generally* Fed. R. Civ. P. 33(d).

**Additional Interrogatory No. 17 (Ms. Jean-Pierre No. 6):**

**Identify all “members of our senior staff” and/or “members of our COVID-19 team” who are “in regular touch with ... social media platforms,” as [Jennifer Psaki] stated at a White House press briefing on or around July 15, 2021, including the nature of the communication and/or coordination.**

**OBJECTIONS:** Defendant incorporates by reference the above objections. Defendant further objects to this Interrogatory on the ground that it is vague because it relies on a characterization of a statement made by an individual no longer in government, and the statement does not specify the individuals at issue or the specific communications referenced. Defendant further objects to this Interrogatory as unduly burdensome and not proportional to the needs of the case. This Request calls for a response based on *any and all* specified “communications” from Defendant or any employee or subordinate of Defendant. Defendants cannot conduct an exhaustive search to uncover all possible responsive information under the current, abbreviated expedited discovery schedule. Defendant also objects to this Interrogatory as overbroad because it calls for a response based on documents that are not relevant to Plaintiffs’ claims and that do not fall within scope of discovery authorized by the Court. The Court authorized the service of discovery requests concerning “the identity of federal officials who have been and are communicating with social-media platforms about [misinformation and] any censorship or suppression of speech on social media, including the nature and content of those communications.” ECF No. 34 at 13. This Interrogatory appears to call for a

**CONFIDENTIAL**

**CONFIDENTIAL**

response based on communications with Social-Media Platforms regardless of whether they pertain to content moderation with respect to misinformation. Defendant also objects to this Interrogatory to the extent it seeks internal, deliberative documents discussing such communications, attorney client documents, or other privileged materials relating to such communications. Defendants also object to this Interrogatory to the extent it seeks information protected by the deliberative process privilege, attorney-client privilege, law enforcement privilege, a statutory national security privilege, presidential communications privilege, or any other applicable privilege. Additionally, challenges to administrative agency action are ordinarily not subject to discovery outside the administrative record. *Lorion*, 470 U.S. at 743-44.

Further, Defendant objects to this Interrogatory on the ground that any discovery on the White House at this stage of the litigation is unduly burdensome and disproportionate to the needs of the case. Plaintiffs have not exhausted all other avenues of discovery before seeking discovery on the White House. *See, e.g.*, Order, *Centro Presente*, No. 1:18-CV-10340 (D. Mass. May 15, 2019); *Karnoski v. Trump*, 926 F.3d 1180, 1207 (9th Cir. 2019); *Cheney*, 542 U.S. at 390. Additionally, discovery propounded on White House officials would create an undue burden, distract them from their critical executive responsibilities, and violate the separation of powers. *See Cheney*, 542 U.S. at 385. That burden is especially undue at this stage of the litigation given that Defendants' motion to dismiss the Amended Complaint for lack of subject-matter jurisdiction and other deficiencies is forthcoming. Additionally, Defendant objects to this request to the extent it is directed to information protected by the presidential communications privilege or other executive privileges. *See Nixon*, 418 U.S. at 708. Because Plaintiffs are not entitled to such information, the request imposes a burden on Defendant disproportionate to the minimal benefit (if any) that Plaintiffs might derive from the possibility of responsive, non-privileged information. *See Cheney*, 542 U.S. at 389.

**CONFIDENTIAL**

**CONFIDENTIAL**

Further, Defendant objects to this Interrogatory as unreasonably cumulative and duplicative of Plaintiffs' Interrogatories 1 through 5, in response to which certain Defendants are producing documents as described herein.

**RESPONSE:** Subject to and without waiving any of the foregoing objections, as amended in accordance with the Court's September 6, 2022, Order, and based on a reasonable inquiry under the circumstances of abbreviated, expedited discovery, the White House Office of the Press Secretary provides the following response:

At a July 15, 2021, press briefing, Ms. Psaki was asked the following question and provided the following response:

Q: Can you talk a little bit more about this request for tech companies to be more aggressive in policing misinformation? Has the administration been in touch with any of these companies and are there any actions that the federal government can take to ensure their cooperation, because we've seen, from the start, there's not a lot of action on some of these platforms.

MS. PSAKI: Well, first, we are in regular touch with these social media platforms, and those engagements typically happen through members of our senior staff, but also members of our COVID-19 team, given, as Dr. Murthy conveyed, this is a big issue of misinformation, specifically on the pandemic.

In terms of actions, Alex, that we have taken — or we're working to take, I should say — from the federal government: We've increased disinformation research and tracking within the Surgeon General's office. We're flagging problematic posts for Facebook that spread disinformation. We're working with doctors and medical professionals to connect — to connect medical experts with popular — with popular — who are popular with their audiences with — with accurate information and boost trusted content. So we're helping get trusted content out there.

We also created the COVID-19 — the COVID Community Corps to get factual information into the hands of local messengers, and we're also investing, as you all have seen in the President's, the Vice President's, and Dr. Fauci's time in meeting with influencers who also have large reaches to a lot of these target audiences who can spread and share accurate information.

You saw an example of that yesterday. I believe that video will be out Fri- — tomorrow. I think that was your question, Steve, yesterday; I did a full follow-up there.

**CONFIDENTIAL**

**CONFIDENTIAL**

There are also proposed changes that we have made to social media platforms, including Facebook, and those specifically are four key steps.

One, that they measure and publicly share the impact of misinformation on their platform. Facebook should provide, publicly and transparently, data on the reach of COVID-19 — COVID vaccine misinformation. Not just engagement, but the reach of the misinformation and the audience that it's reaching.

That will help us ensure we're getting accurate information to people. This should be provided not just to researchers, but to the public so that the public knows and understands what is accurate and inaccurate.

Second, that we have recommended — proposed that they create a robust enforcement strategy that bridges their properties and provides transparency about the rules. So, about — I think this was a question asked before — there's about 12 people who are producing 65 percent of anti-vaccine misinformation on social media platforms. All of them remain active on Facebook, despite some even being banned on other platforms, including Facebook — ones that Facebook owns.

Third, it's important to take faster action against harmful posts. As you all know, information travels quite quickly on social media platforms; sometimes it's not accurate. And Facebook needs to move more quickly to remove harmful, violative posts — posts that will be within their policies for removal often remain up for days. That's too long. The information spreads too quickly.

Finally, we have proposed they promote quality information sources in their feed algorithm. Facebook has repeatedly shown that they have the levers to promote quality information. We've seen them effectively do this in their algorithm over low-quality information and they've chosen not to use it in this case. And that's certainly an area that would have an impact.

So, these are certainly the proposals. We engage with them regularly and they certainly understand what our asks are.

Press Briefing by Press Secretary Jen Psaki and Surgeon General Dr. Vivek H. Murthy, July 15, 2021, available at <https://www.whitehouse.gov/briefing-room/press-briefings/2021/07/15/press-briefing-by-press-secretary-jen-psaki-and-surgeon-general-dr-vivek-h-murthy-july-15-2021/>.

It is the understanding of the White House Office of the Press Secretary (“the Office”) that, in making this statement, Ms. Psaki was referencing the following individuals as “members

**CONFIDENTIAL**

**CONFIDENTIAL**

of our senior staff” or “COVID-19 team” within the White House: Robert Flaherty and Andrew Slavitt.

With respect to the nature of the communications with social media platforms referenced in the July 15 press conference, the Office refers to the full statement quoted above. Ms. Psaki further conveyed her understanding of the nature of such communications in additional statements, including in press conferences on July 16, 2021, and July 19, 2021. Portions of those press conference are quoted below.

Q And just — you went through kind of the topline details of this yesterday, but can you elaborate a little bit on the Facebook —

MS. PSAKI: Sure.

Q — the administration to Facebook flagging of disinformation. And there’s also some reporting that we’ve had that Facebook maybe hasn’t been as proactive as the White House would like it to be in response to some of the flagging. So, the process of how the flagging works, and then whether Facebook has been amenable to those requests.

MS. PSAKI: Sure. Well, I would say first, it shouldn’t come as any surprise that we’re in regular touch with social media platforms — just like we’re in regular touch with all of you and your media outlets — about areas where we have concern, information that might be useful, information that may or may not be interesting to your viewers.

You all make decisions, just like the social media platforms make decisions, even though they’re a private-sector company and different, but just as an example.

So we are ma- — regularly making sure social media platforms are aware of the latest narratives dangerous to public health that we and many other Americans seeing — are seeing across all of social and traditional media. And we work to engage with them to better understand the enforcement of social media platform policies.

So let me give you an example, just to illustrate it a little bit. The false narrative that remains active out there about COVID-19 vaccines causing infertility — something we’ve seen out there, flowing on the internet quite a bit, in other places as well — which has been disproven time and time again. This is troubling, but a persistent narrative that we and many have seen, and we want to know that the social media platforms are taking steps to address it. That is inaccurate, false information.

**CONFIDENTIAL**

**CONFIDENTIAL**

If you are a parent, you would look at that information and then that would naturally raise concerns, but it's inaccurate. And that is an example of the kind of information that we are flagging or raising.

Press Briefing by Press Secretary Jen Psaki, July 16, 2021, available at

<https://www.whitehouse.gov/briefing-room/press-briefings/2021/07/16/press-briefing-by-press-secretary-jen-psaki-july-16-2021/>.

Q Thank you. Will the White House publicly release information on posts that it considers misinformation on vaccines that it's asked Facebook to block?

MS. PSAKI: First of all, we've not asked Facebook to block any individual posts. The way this works is that there are trending — there are trends that are out there on social media platforms. You're aware of them. We're aware of them. Anyone in the public can be aware of them.

There's also data that we look at that many media platforms, like many of you, also look at data in terms of trends and you report on it, which is not — to be expected, given the number of people who get their information from social media.

It's up to social media platforms to determine what their application is of their own rules and regulations. And so we just certainly raise where we have concerns about information that's inaccurate that is traveling out there in whatever platform it's traveling on.

Press Briefing by Press Secretary Jen Psaki, July 19, 2021, available at

<https://www.whitehouse.gov/briefing-room/press-briefings/2021/07/19/press-briefing-by-press-secretary-jen-psaki-july-19-2021/>.

**Additional Interrogatory No. 18 (Ms. Jean-Pierre No. 7):**

**Identify all Communications with any Social-Media Platform relating to “12 people who are producing 65 percent of the anti-vaccine misinformation on social-media platforms,” as [Jennifer Psaki] stated at a White House press briefing on or around July 15, 2021.**

**OBJECTIONS:** Defendant incorporates by reference the above objections. Defendant further objects to this Interrogatory on the ground that it is vague because it relies on a characterization of a statement made by an individual no longer in government, and the statement

**CONFIDENTIAL**

**CONFIDENTIAL**

does not specify the individuals at issue or the specific communications referenced. Defendant further objects to this Interrogatory as unduly burdensome and not proportional to the needs of the case. This Interrogatory calls for a response based on any and all specified documents from Defendant or any employee or subordinate of Defendant. Defendants cannot conduct an exhaustive search to uncover all possible responsive information under the current, abbreviated expedited discovery schedule. Such expedited discovery is especially burdensome given that Defendants' motion to dismiss the Amended Complaint for lack of subject-matter jurisdiction and other deficiencies is forthcoming. Defendant also objects to this Interrogatory as overbroad because it calls for documents that are not relevant to Plaintiffs' claims and that do not fall within scope of discovery authorized by the Court. The Court authorized the service of discovery requests concerning "the identity of federal officials who have been and are communicating with social-media platforms about [misinformation and] any censorship or suppression of speech on social media, including the nature and content of those communications." ECF No. 34 at 13. This Interrogatory appears to call for a response based on communications with Social-Media Platforms regardless of whether they pertain to content moderation with respect to misinformation. Defendants also object to the Interrogatory to the extent a response requires review of internal, deliberative documents discussing such communications, attorney client documents, or other privileged materials relating to agency communications. Defendants also object to this Interrogatory to the extent it seeks information protected by the deliberative process privilege, attorney-client privilege, law enforcement privilege, a statutory national security privilege, presidential communications privilege, or any other applicable privilege. Additionally, challenges to administrative agency action are ordinarily not subject to discovery outside the administrative record. *Lorion*, 470 U.S. at 743-44.

**CONFIDENTIAL**



**CONFIDENTIAL**

Further, Defendant objects to this Interrogatory on the ground that any discovery on the White House at this stage of the litigation is unduly burdensome and disproportionate to the needs of the case. Plaintiffs have not exhausted all other avenues of discovery before seeking discovery on the White House. *See, e.g.*, Order, *Centro Presente*, No. 1:18-CV-10340 (D. Mass. May 15, 2019); *Karnoski v. Trump*, 926 F.3d 1180, 1207 (9th Cir. 2019); *Cheney*, 542 U.S. at 390. Additionally, discovery propounded on White House officials would create an undue burden, distract them from their critical executive responsibilities, and violate the separation of powers. *See Cheney*, 542 U.S. at 385. That burden is especially undue at this stage of the litigation given that Defendants' motion to dismiss the Amended Complaint for lack of subject-matter jurisdiction and other deficiencies is forthcoming. Additionally, Defendant objects to this Interrogatory to the extent it is directed to information protected by the presidential communications privilege or other executive privileges. *See Nixon*, 418 U.S. at 708. Because Plaintiffs are not entitled to such information, the request imposes a burden on Defendant disproportionate to the minimal benefit (if any) that Plaintiffs might derive from the possibility of responsive, non-privileged information. *See Cheney*, 542 U.S. at 389.

Further, Defendant objects to this Interrogatory as unreasonably cumulative and duplicative of Common Interrogatories 1 through 5, in response to which certain Defendants are producing documents as described herein.

**RESPONSE:** Subject to and without waiving any of the foregoing objections, as amended in accordance with the Court's September 6, 2022, Order, and based on a reasonable inquiry under the circumstances of abbreviated, expedited discovery, the White House Office of the Press Secretary provides the following response:

**CONFIDENTIAL**

**CONFIDENTIAL**

The White House Office of the Press Secretary (“the Office”) is unaware of any such communications between employees of the Office and any social media platform that discuss this topic.

**Additional Interrogatory No. 19 (Ms. Jean-Pierre No. 8):**

**On or around July 15, 2021, You stated that “we engage with them [i.e., Social-Media Platforms] regularly and they certainly understand what our asks are.” Identify what Social-Media Platform(s) are included in any such engagement(s), and identify “what our asks are,” including Communication(s) relating to such engagement(s) and ask(s).**

**OBJECTIONS:** Defendant incorporates by reference the above objections. Defendant further objects to this Interrogatory on the ground that it is vague because it relies on a characterization of a statement made by an individual no longer in government, and the statement does not specify the individuals at issue or the specific communications referenced. Defendant further objects to this Interrogatory as unduly burdensome and not proportional to the needs of the case. This Interrogatory calls for a response based on any and all specified documents from Defendant or any employee or subordinate of Defendant. Defendants cannot conduct an exhaustive search to uncover all possible responsive information under the current, abbreviated expedited discovery schedule. Such expedited discovery is especially burdensome given that Defendants’ motion to dismiss the Amended Complaint for lack of subject-matter jurisdiction and other deficiencies is forthcoming. Defendant also objects to this Interrogatory as overbroad because it calls for documents that are not relevant to Plaintiffs’ claims and that do not fall within scope of discovery authorized by the Court. The Court authorized the service of discovery requests concerning “the identity of federal officials who have been and are communicating with social-media platforms about [misinformation and] any censorship or suppression of speech on social media, including the nature and content of those communications.” ECF No. 34 at 13. This Interrogatory appears to call for a response based on communications with Social-Media Platforms

**CONFIDENTIAL**

**CONFIDENTIAL**

regardless of whether they pertain to content moderation with respect to misinformation. Defendants also object to the Interrogatory to the extent a response requires review of internal, deliberative documents discussing such communications, attorney client documents, or other privileged materials relating to agency communications. Defendants also object to this Interrogatory to the extent it seeks information protected by the deliberative process privilege, attorney-client privilege, law enforcement privilege, a statutory national security privilege, presidential communications privilege, or any other applicable privilege. Additionally, challenges to administrative agency action are ordinarily not subject to discovery outside the administrative record. *Lorion*, 470 U.S. at 743-44.

Further, Defendant objects to this Interrogatory on the ground that any discovery on the White House at this stage of the litigation is unduly burdensome and disproportionate to the needs of the case. Plaintiffs have not exhausted all other avenues of discovery before seeking discovery on the White House. *See, e.g.*, Order, *Centro Presente*, No. 1:18-CV-10340 (D. Mass. May 15, 2019); *Karnoski v. Trump*, 926 F.3d 1180, 1207 (9th Cir. 2019); *Cheney*, 542 U.S. at 390. Additionally, discovery propounded on White House officials would create an undue burden, distract them from their critical executive responsibilities, and violate the separation of powers. *See Cheney*, 542 U.S. at 385. That burden is especially undue at this stage of the litigation given that Defendants' motion to dismiss the Amended Complaint for lack of subject-matter jurisdiction and other deficiencies is forthcoming. Additionally, Defendant objects to this Interrogatory to the extent it is directed to information protected by the presidential communications privilege or other executive privileges. *See Nixon*, 418 U.S. at 708. Because Plaintiffs are not entitled to such information, the request imposes a burden on Defendant disproportionate to the minimal benefit

**CONFIDENTIAL**

**CONFIDENTIAL**

(if any) that Plaintiffs might derive from the possibility of responsive, non-privileged information. See *Cheney*, 542 U.S. at 389.

Further, Defendant objects to this Interrogatory as unreasonably cumulative and duplicative of Common Interrogatories 1 through 5, in response to which certain Defendants are producing documents as described herein.

**RESPONSE:** Subject to and without waiving any of the foregoing objections, as amended in accordance with the Court’s September 6, 2022, Order, and based on a reasonable inquiry under the circumstances of abbreviated, expedited discovery, the White House Office of the Press Secretary provides the following response:

It is the understanding of the White House Office of the Press Secretary (the “Office”) that, in referring to individuals who “engaged with them [i.e., social-media platforms],” Ms. Psaki was not referring to employees of the Office. It is the understanding of the Office that the social media platforms referenced in this statement include, but are not necessarily limited to, Facebook and YouTube. With respect to “what our asks are,” the Office refers to Ms. Psaki’s statements, set forth above in response to Interrogatory 17, in which she conveyed her understanding of the nature of the “engagement(s)” or “ask(s).” The Office is unaware of any communications between employees of the Office and any social media platform that discuss this topic.

**Additional Interrogatory No. 20 (Ms. Jean-Pierre No. 10):**

**Identify all person(s) who “engage[s] regularly with all social media platforms about steps that can be taken” to address Misinformation on social media, which engagement “has continued, and ... will continue,” as You stated at the April 25, 2022 White House press briefing, including all Communications with any Social-Media Platform involved in such engagement.**

**OBJECTIONS:** Defendant incorporates by reference the above objections. Defendant further objects to this Interrogatory on the ground that it is vague because it relies on a

**CONFIDENTIAL**

**CONFIDENTIAL**

characterization of a statement made by an individual no longer in government, and the statement does not specify the individuals at issue or the specific communications referenced. Defendant further objects to this Interrogatory as unduly burdensome and not proportional to the needs of the case. This Interrogatory calls for a response based on any and all specified documents from Defendant or any employee or subordinate of Defendant. Defendants cannot conduct an exhaustive search to uncover all possible responsive information under the current, abbreviated expedited discovery schedule. Such expedited discovery is especially burdensome given that Defendants' motion to dismiss the Amended Complaint for lack of subject-matter jurisdiction and other deficiencies is forthcoming. Defendant also objects to this Interrogatory as overbroad because it calls for documents that are not relevant to Plaintiffs' claims and that do not fall within scope of discovery authorized by the Court. The Court authorized the service of discovery requests concerning "the identity of federal officials who have been and are communicating with social-media platforms about [misinformation and] any censorship or suppression of speech on social media, including the nature and content of those communications." ECF No. 34 at 13. This Interrogatory appears to call for a response based on communications with Social-Media Platforms regardless of whether they pertain to content moderation with respect to misinformation. Defendants also object to the Interrogatory to the extent a response requires review of internal, deliberative documents discussing such communications, attorney client documents, or other privileged materials relating to agency communications. Defendant also objects to this Request to the extent it seeks internal, deliberative documents discussing such communications, attorney client documents, or other privileged materials relating to such communications. Defendants also object to this Interrogatory to the extent it seeks information protected by the deliberative process privilege, attorney-client privilege, law enforcement privilege, a statutory national security

**CONFIDENTIAL**

**CONFIDENTIAL**

privilege, presidential communications privilege, or any other applicable privilege. Additionally, challenges to administrative agency action are ordinarily not subject to discovery outside the administrative record. *Lorion*, 470 U.S. at 743-44.

Further, Defendant objects to this Interrogatory on the ground that any discovery on the White House at this stage of the litigation is unduly burdensome and disproportionate to the needs of the case. Plaintiffs have not exhausted all other avenues of discovery before seeking discovery on the White House. *See, e.g.*, Order, *Centro Presente*, No. 1:18-CV-10340 (D. Mass. May 15, 2019); *Karnoski v. Trump*, 926 F.3d 1180, 1207 (9th Cir. 2019); *Cheney*, 542 U.S. at 390. Additionally, discovery propounded on White House officials would create an undue burden, distract them from their critical executive responsibilities, and violate the separation of powers. *See Cheney*, 542 U.S. at 385. That burden is especially undue at this stage of the litigation given that Defendants' motion to dismiss the Amended Complaint for lack of subject-matter jurisdiction and other deficiencies is forthcoming. Additionally, Defendant objects to this Interrogatory to the extent it is directed to information protected by the presidential communications privilege or other executive privileges. *See Nixon*, 418 U.S. at 708. Because Plaintiffs are not entitled to such information, the request imposes a burden on Defendant disproportionate to the minimal benefit (if any) that Plaintiffs might derive from the possibility of responsive, non-privileged information. *See Cheney*, 542 U.S. at 389.

Further, Defendant objects to this Interrogatory as unreasonably cumulative and duplicative of Common Interrogatories 1 through 5, in response to which certain Defendants are producing documents as described herein.

**RESPONSE:** Subject to and without waiving any of the foregoing objections, as amended in accordance with the Court's September 6, 2022, Order, and based on a reasonable inquiry under

**CONFIDENTIAL**

**CONFIDENTIAL**

the circumstances of abbreviated, expedited discovery, the White House Office of the Press Secretary provides the following response:

At an April 25, 2022, press briefing, Ms. Psaki was asked the following questions and provided the following responses:

Q Jen, the Surgeon General has said that misinformation about COVID amounts to a public health crisis.

MS. PSAKI: Yeah.

Q I'm wondering: Regardless of ownership, would the White House be interested in working with Twitter like it has in the past to continue to combat this kind of misinformation? Or are we in a different part of the pandemic where that kind of partnership is no longer necessary?

MS. PSAKI: Well, I think we engage regularly with all social media platforms about steps that can be taken that has continued, and I'm sure it will continue. But there are also reforms that we think Congress could take and we would support taking, including reforming Section 230, enacting antitrust reforms, requiring more transparency. And the President is encouraged by the bipartisan support for — or engagement in those efforts.

Press Briefing by Press Secretary Jen Psaki, April 25, 2022, available at

<https://www.whitehouse.gov/briefing-room/press-briefings/2022/04/25/press-briefing-by-press-secretary-jen-psaki-april-25-2022/>.

The White House Office of the Press Secretary (“the Office”) understands the “engage[ments]” in this statement to refer to “engage[ments]” about COVID-19 misinformation. Accordingly, the Office incorporates by reference its response to Interrogatory No. 17 above. The Office is unaware of any communications between employees of the Office and any social media platform that discuss this topic.

**CONFIDENTIAL**

**CONFIDENTIAL**

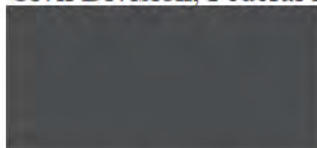
Dated: September 27, 2022

Respectfully submitted,

BRIAN M. BOYNTON  
Principal Deputy Assistant Attorney General

JAMES J. GILLIGAN  
Special Litigation Counsel, Federal Programs Branch

/s/ Kyla Snow  
ADAM D. KIRSCHNER (IL Bar No. 6286601)  
Senior Trial Counsel  
KYLA SNOW (OH Bar No. 96662)  
INDRANEEL SUR (D.C. Bar No. 978017)  
KUNTAL CHOLERA (D.C. Bar No. 1031523)  
Trial Attorneys  
U.S. Department of Justice  
Civil Division, Federal Programs Branch



*Attorneys for Defendants*

**CONFIDENTIAL**



### Verification

I, Samantha Vinograd, hereby declare that I am the Acting Assistant Secretary of Homeland Security for Counterterrorism, Threat Prevention, and Law Enforcement Policy at the Department of Homeland Security. Based on reasonable inquiry and information provided to me in my official capacity, pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury that the information regarding the Department of Homeland Security contained in the Defendants' responses to Plaintiff's Common Interrogatories 1–5 and Additional Interrogatories 8–14 is true and correct to the best of my knowledge.

SAMANTHA E  
VINOGRAD

---

Digitally signed by SAMANTHA  
E VINOGRAD  
Date: 2022.08.17 18:17:25  
-04'00'

Samantha Vinograd

Acting Assistant Secretary of Homeland Security for  
Counterterrorism, Threat Prevention, and Law Enforcement Policy

Department of Homeland Security

**VERIFICATION**

I, Geoffrey Hale, pursuant to 28 U.S.C. § 1746, declare under penalty of perjury that the interrogatory response of the Cybersecurity and Infrastructure Security Agency to Plaintiffs' First Set of Expedited Preliminary-Injunction Related Interrogatories dated July 18, 2022, Common Interrogatories Numbers 1-5 and Additional Interrogatories Numbers 15 and 16, contained in the Responses of the Cybersecurity and Infrastructure Security Agency, is true and correct, to the best of my knowledge.

Dated: August 16, 2022



---


Geoffrey Hale  
Lead of Election Security & Resilience  
Cybersecurity and Infrastructure Security Agency

**VERIFICATION**

I, Carol Crawford, pursuant to 28 U.S.C. § 1746, declare under penalty of perjury that the interrogatory response of the Centers for Disease Control and Prevention to Plaintiffs’ First Set of Expedited Preliminary-Injunction Related Interrogatories dated July 18, 2022, Common Interrogatories Numbers 1-5 and Additional Interrogatories Numbers 1-4 contained in the Responses of the Centers for Disease Control and Prevention, is true and correct, to the best of my knowledge.

Dated: August 17, 2022

Carol  
Crawford -S



Digitally signed by  
Carol Crawford -S  
Date: 2022.08.17  
17:20:13 -04'00'

---

Carol Crawford  
Health Communications Specialist  
Director, Division of Digital Media, OADC  
Centers for Disease Control and Prevention

**VERIFICATION**

I, Max Lesko, pursuant to 28 U.S.C. § 1746, declare under penalty of perjury that the amended interrogatory response of the Office of the Surgeon General to Plaintiffs' First Set of Expedited Preliminary-Injunction Related Interrogatories dated July 18, 2022, Common Interrogatories Numbers 1-5 and Additional Interrogatories Numbers 1-3, contained in the Responses of the Office of the Surgeon General, is true and correct, to the best of my knowledge.

Dated: September 27, 2022



Max Lesko

Chief of Staff

Office of the Surgeon General

**VERIFICATION**

I, Jill R. Harper, Ph.D., pursuant to 28 U.S.C. § 1746, declare under penalty of perjury that the amended interrogatory response of the National Institute of Allergy and Infectious Diseases, including of Dr. Fauci in his roles as Director of NIAID and as Chief Medical Advisor to the President, to Plaintiffs' First Set of Expedited Preliminary-Injunction Related Interrogatories dated July 18, 2022, Common Interrogatories Numbers 1-5 and Additional Interrogatories Numbers 1, 3, and 5-7, contained in the Responses of the National Institute of Allergy and Infectious Diseases, is true and correct, to the best of my knowledge.

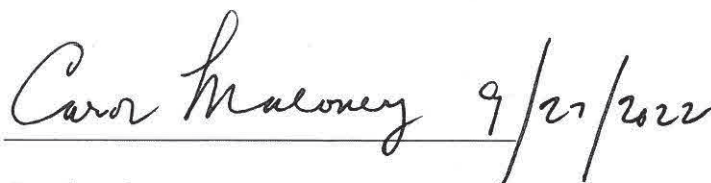
Dated: September 27, 2022

**Jill R. Harper** Digitally signed by Jill R. Harper -S  
-S Date: 2022.09.27 12:46:40 -04'00'

Jill R. Harper, Ph.D.  
Deputy Director for Science Management,  
and Executive Officer  
NIAID/NIH/DHHS

**VERIFICATION**

I, Carol Maloney, pursuant to 28 U.S.C. § 1746, declare under penalty of perjury that the interrogatory response of the four current and former employees of the United States Department of Health and Human Services (HHS) identified in the Court's September 6, 2022 Order to Plaintiffs' First Set of Expedited Preliminary-Injunction Related Interrogatories dated July 18, 2022, Common Interrogatories Numbers 1-5 and Additional Interrogatories Number 1-3, is true and correct, to the best of my knowledge.



Carol Maloney  
Executive Director/Deputy Agency Chief FOIA Officer  
Office of the Assistant Secretary of Public Affairs

**VERIFICATION**

I, Robert E. Dornbush III, pursuant to 28 U.S.C. § 1746, declare under penalty of perjury that the interrogatory response of the Office of the Press Secretary to Plaintiffs' First Set of Expedited Preliminary-Injunction Related Interrogatories dated July 18, 2022, Common Interrogatories Numbers 1-5 and Additional Interrogatories Numbers 17-20, contained in the Responses of the Office of the Press Secretary, is true and correct, to the best of my knowledge.

Dated: September 27, 2022



Robert E. Dornbush III  
Chief of Staff and Special Assistant to the Press Secretary  
Office of the Press Secretary

**From:** [REDACTED]@fb.com]  
**Sent:** 9/16/2020 2:17:55 PM  
**To:** Masterson, Matthew [REDACTED]@cisa.dhs.gov]; Scully, Brian [REDACTED]@cisa.dhs.gov]  
**CC:** Snell, Allison [REDACTED]@cisa.dhs.gov]; Hale, Geoffrey [REDACTED]@cisa.dhs.gov]; [REDACTED]  
[REDACTED]@fb.com]  
**Subject:** Today's industry statement

**CAUTION:** This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Gents,

Apologize for the late sharing of the statement below, but wanted to ensure you had the statement we will look to release following today's meeting.

Many thanks-- as always --for your partnership.

Best,  
Sandy

#### JOINT INDUSTRY STATEMENT:

"For several years, tech companies have worked together, and with U.S. government agencies tasked with protecting the integrity of elections, to counter election threats across our respective platforms. As we approach the November election, we continue to prepare, meet regularly, and share updates on the threats we see. At today's meeting, we specifically discussed:

1. Ways to help provide real-time, clear information about the voting process and election results given expected logistical disruptions posed by COVID-19.
2. Ways to counter targeted attempts to undermine the election conversation before, during, and after the election. This includes preparing for possible so-called "hack and leak" operations attempting to use platforms and traditional media to amplify unauthorized information drops.
3. Detection efforts for potential cyberattacks targeting campaigns, voting agencies, and agencies responsible for voting infrastructure.

As the global pandemic poses unprecedented challenges for the 2020 U.S. election, we will continue this ongoing communication and close work between industry and U.S. institutions tasked with election security to share key findings and operational insights in the weeks to come."

Can confirm:

Among participants in today's industry-government meeting were: Google, Microsoft, Facebook, Twitter, Reddit, Verizon Media, Pinterest, LinkedIn, Wikimedia Foundation, the Cybersecurity and Infrastructure Security Agency (CISA), the FBI's Foreign Influence Task Force, DOJ's National Security Division, and the Office of the Director of National Intelligence (ODNI).





**From:** Protentis, Lauren [/O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=604C2D8C37944283805D4BD9A9A83476-LAUREN.PROT]  
**Sent:** 4/19/2022 9:45:23 AM  
**To:** [REDACTED]@fb.com]; [REDACTED]@fb.com]; [REDACTED]@fb.com]  
**Subject:** Agenda for April Industry/USG Sync

Hi All,

Sharing the agenda for tomorrow's call. We won't be having a discussion on DHS organizational changes this month, we will likely do that in May.

1. Opening (Facilitator: Lauren)
  - a. Roll Call: CISA, FBI, DNI, DHS
  - b. One-Pager Reminder
2. Government Meeting Topics (Facilitator: Lauren) w
  - a. Information Sharing Around Elections Risk (CISA: Hale, DNI: [REDACTED] FBI: Demlow, DHS: Beckman)
    - i. CISA: Infrastructure Risks
    - ii. DHS I&A: Infrastructure Activity
    - iii. DNI: Geopolitical Considerations
    - iv. FBI: Other
3. Industry Meeting Topics (Facilitator: Meta)

Lauren Protentis (She/Her)  
 Mis, Dis, and Mal-information (MDM) Team  
 Election Security Initiative  
 National Risk Management Center  
 Cybersecurity and Infrastructure Security Agency  
 O: [REDACTED] | Email: [REDACTED]@cisa.dhs.gov | HSDN: [REDACTED]@dhs.sgov.gov | CLAN:  
 [REDACTED]@dhs.ic.gov



**From:** Protentis, Lauren [/O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=604C2D8C37944283805D4BD9A9A83476-LAUREN.PROT]  
**Sent:** 7/20/2022 10:16:12 AM  
**To:** [REDACTED]@fb.com]; [REDACTED]@fb.com]; [REDACTED]@fb.com]  
**CC:** [REDACTED]@fb.com]  
**Subject:** Agenda: USG | Industry Call

Hi All,

Looking forward to connecting today, I pulled the agenda together below for today's call. Let me know if you have any questions.

1. Opening (Facilitator: Lauren)
2. Government Meeting Topics (Facilitator: Lauren)
- b. Information Sharing Around Elections Risk
  - i. **Annotation – Industry Prompts:**
    1. (1) Races/states that you anticipate may be particularly targeted; (2) Themes/narratives/approaches you anticipate for races that you think will be targeted; (3) Specific indicators about infrastructure that foreign actors could use to target US; (4) Specific dates/events within the electoral calendar that you anticipate may be targeted; (5) May still be too early for this, but on inter-related risk between Ukraine and the US: does the developing situation increase (or decrease?) the risk that Russia may target the midterms?
  - ii. **Annotation – Briefing Structure**
    4. CISA – Elections Infrastructure Risks (Scully)
    5. DHS I&A – Infrastructure Activity (Beckman)
    6. FBI – Domestic Adversarial Actor Update (Dehmlow)
    7. DNI – Geopolitical Considerations ([REDACTED])
3. Industry Meeting Topics (Facilitator: Meta)
  - a. Industry Briefs
  - i. **Annotation – USG Prompts:**
    - i. To what extent have you identified notable commonalities/differences between how foreign actors seek to use social media to influence their expatriate populations within the US on elections/other topics of strategic interest versus the broader US public? What stands out?
    - ii. Do you and to what extent assess that foreign actors display greater willingness to directly engage US political entities, US activists, and US media organizations that fall within diaspora communities? Do these engagements stand out to you or do you judge them as largely consistent with steady state foreign influence behavior across target audiences?
    - iii. To what extent or degree do you assess that PRC-linked or pro-CCP online influencers are amplifying divisive social and political issues in the United States?

Lauren Protentis (She/Her)  
 Mis, Dis, and Mal-information (MDM) Team  
 Election Security Initiative  
 National Risk Management Center  
 Cybersecurity and Infrastructure Security Agency  
 O: [REDACTED] | Email: [REDACTED]@cisa.dhs.gov | HSDN: [REDACTED]@dhs.sgov.gov | CLAN:  
 [REDACTED]@dhs.ic.gov

**From:** Protentis, Lauren [/O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=604C2D8C37944283805D48D9A9A83476-LAUREN.PROT]  
**Sent:** 4/14/2022 12:52:23 PM  
**To:** [REDACTED]@fb.com]; [REDACTED]@fb.com]; Schaul, Robert [REDACTED]@cisa.dhs.gov]; Senninger, Marcus [REDACTED]@cisa.dhs.gov]; Wyman, Kim (She/Her/Hers) [REDACTED]@cisa.dhs.gov]; Hale, Geoffrey (He/Him) [REDACTED]@cisa.dhs.gov]; Snell, Allison (She/Her) [REDACTED]@cisa.dhs.gov]; [REDACTED]@fb.com]; [REDACTED]@fb.com]; Scully, Brian [REDACTED]@cisa.dhs.gov]  
**CC:** [REDACTED]@fb.com]  
**Subject:** RE: [Prep] USG | Industry Call (Monthly)

Hi All,

Sharing a tentative agenda for next week's USG/Industry Sync. Looking forward to discussing at 1:00.

March USG | Industry Call Annotated Agenda

1. Opening (Facilitator: Lauren)
  - a. Roll Call: CISA, FBI, DNI, DHS
  - b. One-Pager Reminder
2. Government Meeting Topics (Facilitator: Lauren)
  - a. DHS Brief (Tentative)
  - b. Information Sharing Around Elections Risk (CISA: Hale, DNI: [REDACTED] FBI: Demlow/Criminal Investigative Unit, DHS: Beckman)
- i. **Industry Prompts:**
  1. (1) Races/states that you anticipate may be particularly targeted; (2) Themes / narratives / approaches you anticipate for races that you think will be targeted; (3) Specific indicators about infrastructure that foreign actors could use to target US; (4) Specific dates / events within the electoral calendar that you anticipate may be targeted; (5) May still be too early for this, but on inter-related risk between Ukraine and the US: does the developing situation increase (or decrease?) the risk that Russia may target the midterms?
3. Industry Meeting Topics (Facilitator: Meta)

Lauren Protentis (She/Her)  
 Mis, Dis, and Mal-information (MDM) Team  
 Election Security Initiative  
 National Risk Management Center  
 Cybersecurity and Infrastructure Security Agency  
 O: [REDACTED] | Email: [REDACTED]@cisa.dhs.gov | HSDN: [REDACTED]@dhs.gov | CLAN: [REDACTED]@dhs.ic.gov



-----Original Appointment-----

**From:** [REDACTED]@fb.com>  
**Sent:** Tuesday, March 29, 2022 5:30 PM  
**To:** [REDACTED]; [REDACTED]; Protentis, Lauren; Schaul, Robert; Senninger, Marcus; Wyman, Kim (She/Her/Hers); Hale, Geoffrey (He/Him); Snell, Allison (She/Her); [REDACTED] [REDACTED]  
**Cc:** [REDACTED]  
**Subject:** [Prep] USG | Industry Call (Monthly)

**When:** Thursday, April 14, 2022 10:00 AM-10:30 AM (UTC-08:00) Pacific Time (US & Canada).

**Where:** <https://fb.zoom.us/j/97641435542?pwd=KzNWU0c2dHRME53SHFpSFdYdk4wZz09>

**CAUTION:** This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

One-off prep meetings scheduled on Thursday due to calendar conflicts

**Prep Mtg** – Occurs the 2<sup>nd</sup> Wednesday monthly

WAYS TO JOIN

Join Zoom Meeting

[Redacted]

Meeting ID:

[Redacted]

Passcode: 09

[Redacted]

One tap Mobile

+1 [Redacted] # US (San Jose)

+1 [Redacted] # US (San Jose)

Dial by your location

toll: +1 [Redacted] (San Jose US)

toll: +1 [Redacted] (New York US)

toll: +1 [Redacted] (Providence RI)

toll: +1 [Redacted] (Washington DC US)

toll: +1 [Redacted] (Chicago US)

toll: +1 [Redacted] (Houston US)

tollfree: [Redacted] (US)

tollfree: [Redacted] (US)

tollfree: [Redacted] (US)

tollfree: [Redacted] (US)

Meeting [Redacted]

Passcode: [Redacted]

**Sent:** 8/11/2020 2:13:42 PM  
**To:** [REDACTED]@fb.com]; Scully, Brian [REDACTED]@cisa.dhs.gov]  
**CC:** [REDACTED]@fb.com]; [REDACTED]@fb.com]  
**Subject:** RE: Draft August 2020 Agenda for USG/Industry Meeting

[REDACTED] thanks. I know WSJ reached out for comment but not sur

Matthew V. Masterson  
 Senior Cybersecurity Advisor  
 Department of Homeland Security  
 Cybersecurity & Infrastructure Security Agency (CISA)  
 [REDACTED]  
 [REDACTED]@hq.dhs.gov

**From:** [REDACTED]@fb.com>  
**Sent:** Tuesday, August 11, 2020 2:12 PM  
**To:** Masterson, Matthew [REDACTED]@cisa.dhs.gov>; Scully, Brian [REDACTED]@cisa.dhs.gov>  
**Cc:** [REDACTED]@fb.com>; [REDACTED]@fb.com>  
**Subject:** Re: Draft August 2020 Agenda for USG/Industry Meeting

Matt,

Thanks for the quick reply and for forwarding to your partners.

On your other question, our desire to make a statement has been in the "works" for a while—it just took us time to coalesce and pull it together. Bottom line--we have wanted to highlight all the good work we have done together; it is It is unrelated to the WSJ story.

**From:** "[REDACTED]@cisa.dhs.gov" <[REDACTED]@cisa.dhs.gov>  
**Date:** Tuesday, August 11, 2020 at 1:58 PM  
**To:** [REDACTED]@fb.com>, [REDACTED]@cisa.dhs.gov>  
**Cc:** [REDACTED]@fb.com>, [REDACTED]@fb.com>  
**Subject:** RE: Draft August 2020 Agenda for USG/Industry Meeting

Thanks Sandy. We will share with our Gov't partners. Is this being offered in part because of WSJ outreach? I spoke off the record with the reporter and reinforced the good work we are all doing.

Matthew V. Masterson  
 Senior Cybersecurity Advisor  
 Department of Homeland Security  
 Cybersecurity & Infrastructure Security Agency (CISA)  
 [REDACTED]  
 [REDACTED]@hq.dhs.gov

**From:** [REDACTED]@fb.com>  
**Sent:** Tuesday, August 11, 2020 1:56 PM  
**To:** Masterson, Matthew <[REDACTED]@cisa.dhs.gov>; Scully, Brian <[REDACTED]@cisa.dhs.gov>  
**Cc:** [REDACTED]@fb.com>; [REDACTED]@fb.com>  
**Subject:** Re: Draft August 2020 Agenda for USG/Industry Meeting

Gents,

Hope you are doing well. We saw your email about the Clemson researchers and are taking a look and will come back on that. Appreciate your sharing and advocacy there.

In the meantime, we wanted to share for awareness that tomorrow after our USG/Industry meeting, the industry side will be releasing the below statement (close hold/under embargo until released), and we wanted to let you know in case you would like to share with the other USG participants?

Separately, would it be possible for DNI attendees on the call to share more detail and color around the Evanina statement released last week? Many of our industry attendees are keen to hear and learn more about this tomorrow during our meeting: <https://www.dni.gov/index.php/newsroom/press-releases/item/2139-statement-by-ncsc-director-william-evanina-election-threat-update-for-the-american-public>

Thanks so much, and see you tomorrow!

[REDACTED]

### Joint industry statement:

"For the past several years, we have worked closely to counter information operations across our platforms. We have collaborated in preparation for the upcoming election and regularly meet to discuss trends with U.S. government agencies tasked with protecting the integrity of the election. We held the latest in a series of meetings with government partners today where we each provided updates on what we're seeing on our respective platforms and what we expect to see in the coming months. Specifically, we discussed preparations for the upcoming conventions and scenario planning related to election results. We will continue to stay vigilant on these issues and meet regularly ahead of the November election."

### Background:

- Since 2018, the tech industry and U.S. government agencies tasked with protecting the integrity of the election have been regularly meeting to discuss election security and ways to counter information operations across the Internet.
- Among participants in today's industry-government meeting were: Google, Facebook, Twitter, Reddit, Microsoft, Verizon Media, Pinterest, LinkedIn, the Cybersecurity and Infrastructure Security Agency (CISA), the FBI's Foreign Influence Task Force, DOJ's National Security Division, and the Office of the Director of National Intelligence (ODNI).

---

**From:** [REDACTED]@fb.com>  
**Date:** Friday, August 7, 2020 at 8:57 AM  
**To:** Matthew Masterson [REDACTED]@hq.dhs.gov>, "Scully, Brian" [REDACTED]@cisa.dhs.gov>  
**Cc:** "Snell, Allison" [REDACTED]@hq.dhs.gov>, [REDACTED]@cisa.dhs.gov" <[REDACTED]@cisa.dhs.gov>, [REDACTED]@fb.com>, [REDACTED]@fb.com>  
**Subject:** Draft August 2020 Agenda for USG/Industry Meeting

Brian & Matt,

Provided below is industry's proposed agenda for next week's meeting. Let us know if you have any questions.

Best,

[https://docs.google.com/presentation/d/1LoYEnP1AJCId924OLXH4PXnTweGmMEopJGI\\_D1xNj5M/edit#slide=id.g84d100c656\\_0\\_0](https://docs.google.com/presentation/d/1LoYEnP1AJCId924OLXH4PXnTweGmMEopJGI_D1xNj5M/edit#slide=id.g84d100c656_0_0)

#### August 2020 USG/Industry Meeting

- 10 minutes: Dial In/Opening
  - 30 minutes: Threat Updates
    - Threat update from USG (FBI, I&A)
    - Threat update from industry (TW, FB, GOOG)
  - 40 minutes: Deep Dive Topics (Industry/USG Moderated Discussion)
    - Election process update from USG (Vote-by-Mail, Polling Places, Poll Workers, and Election Results)
    - Threat Landscape in Advance of the Conventions & Debates
    - Election Day Coordination
  - 10 minutes: Highlights & Upcoming Watch Outs & Wrap (Moderated)

**From:** [REDACTED]@fb.com]  
**Sent:** 3/16/2022 2:20:52 AM  
**To:** Protentis, Lauren [REDACTED]@cisa.dhs.gov]; [REDACTED]@fb.com]; [REDACTED]@fb.com]; Snell, Allison (She/Her) [REDACTED]@cisa.dhs.gov]; Hale, Geoffrey (He/Him) [REDACTED]@cisa.dhs.gov]; Schaul, Robert [REDACTED]@cisa.dhs.gov]; Senninger, Marcus [REDACTED]@cisa.dhs.gov]; Wyman, Kim (She/Her/Hers) [REDACTED]@cisa.dhs.gov]; Steven Siegel [REDACTED]@fb.com]  
**Subject:** Re: [PREP] USG | Industry Call (Bi-Monthly)

Hey Lauren,

One more follow-up: do you have a particular email you'd like us to send info about account security steps that elections officials can take from the different companies? When we discussed, we concluded the easiest path would be for each of the companies to send along their one-pagers with protection programs directly. Should I tell them to send to you? Or is there another recipient that would work better?

Best,

[Get Outlook for iOS](#)

**From:** [REDACTED]@fb.com>  
**Sent:** Monday, March 14, 2022 12:43:36 PM  
**To:** Protentis, Lauren <[REDACTED]@cisa.dhs.gov>; [REDACTED]@fb.com> [REDACTED]@fb.com>; Snell, Allison (She/Her) [REDACTED]@cisa.dhs.gov>; Hale, Geoffrey (He/Him) [REDACTED]@cisa.dhs.gov>; Schaul, Robert [REDACTED]@cisa.dhs.gov>; Senninger, Marcus [REDACTED]@cisa.dhs.gov>; Wyman, Kim (She/Her/Hers) [REDACTED]@cisa.dhs.gov>; [REDACTED]@fb.com>  
**Subject:** Re: [PREP] USG | Industry Call (Bi-Monthly)

Thank you for the reminder --

Key questions about the upcoming midterms:

1. Races/states that you anticipate may be particularly targeted;
2. Themes / narratives / approaches you anticipate for races that you think will be targeted;
3. Specific indicators about infrastructure that foreign actors could use to target US;
4. Specific dates / events within the electoral calendar that you anticipate may be targeted (we've asked this before, so primarily any updates on previous prezos);
5. May still be too early for this, but on inter-related risk between Ukraine and the US: does the developing situation increase (or decrease?) the risk that Russia may target the midterms?

Also, industry is supportive of shifting to monthly following this meeting!

N

**From:** Protentis, Lauren [REDACTED]@cisa.dhs.gov>  
**Sent:** Monday, March 14, 2022 12:33 PM



To: [redacted]@fb.com>; [redacted]@fb.com>; [redacted]@fb.com>; Snell, Allison (She/Her) <[redacted]@cisa.dhs.gov>; Hale, Geoffrey (He/Him) <[redacted]@cisa.dhs.gov>; Schaul, Robert <[redacted]@cisa.dhs.gov>; Senninger, Marcus <[redacted]@cisa.dhs.gov>; Wyman, Kim (She/Her/Hers) <[redacted]@cisa.dhs.gov>; [redacted]@fb.com>  
Subject: RE: [PREP] USG | Industry Call (Bi-Monthly)

Hope you had a great weekend.

Wanted to circle back on this so we can give DNI, FBI, DHS some ideas for scoping their remarks for Wednesday 😊!

Let me know if you have any questions!

Lauren Protentis (She/Her)  
Mis, Dis, and Mal-information (MDM) Team  
Election Security Initiative  
National Risk Management Center  
Cybersecurity and Infrastructure Security Agency

O: [redacted] Email: [redacted]@cisa.dhs.gov | HSDN: [redacted]@dhs.gov | CLAN: [redacted]@dhs.ic.gov



---

From: Protentis, Lauren <[redacted]@cisa.dhs.gov>  
Sent: Friday, March 11, 2022 1:18 PM  
To: [redacted]@fb.com>; [redacted]@fb.com>; [redacted]@fb.com>; Snell, Allison (She/Her) <[redacted]@cisa.dhs.gov>; Hale, Geoffrey (He/Him) <[redacted]@cisa.dhs.gov>; Schaul, Robert <[redacted]@cisa.dhs.gov>; Senninger, Marcus <[redacted]@cisa.dhs.gov>; Wyman, Kim (She/Her/Hers) <[redacted]@cisa.dhs.gov>; [redacted]@fb.com>  
Subject: Re: [PREP] USG | Industry Call (Bi-Monthly)

Happy Friday,

Thanks for the productive call on Wednesday. Curious if you collected any questions (specific to risks to the Midterms) from the industry side that I can share with the USG in advance of next weeks call?

Thanks so much!  
Lauren

Lauren Protentis • Mis, Dis, Malinformation Team • National Risk Management Center • Cybersecurity and Infrastructure Security Agency (CISA)

M: [redacted] | E: [redacted]@cisa.dhs.gov | HSDN: [redacted]@dhs.gov | CLAN: [redacted]@dhs.ic.gov



**From:** Protentis, Lauren

**Sent:** Wednesday, March 9, 2022 1:21:44 PM

**To:** [REDACTED]@fb.com>; [REDACTED]@fb.com>; [REDACTED]@fb.com>; Snell, Allison (She/Her) [REDACTED]@cisa.dhs.gov>; Hale, Geoffrey (He/Him) [REDACTED]@cisa.dhs.gov>; Schaul, Robert [REDACTED]@cisa.dhs.gov>; Senninger, Marcus <[REDACTED]@cisa.dhs.gov>; Wyman, Kim (She/Her/Hers) [REDACTED]@cisa.dhs.gov>; [REDACTED]@fb.com>

**Subject:** RE: [PREP] USG | Industry Call (Bi-Monthly)

Hi All,

Sharing a tentative agenda, for your review, for next week's call. Looking forward to our call at 2:00.

1. Opening (Facilitator: CISA)
  - a. Roll Call: FBI, DNI, DHS
  - b. Housekeeping Notes
2. Government Meeting Topics (Facilitator: CISA)
  - a. Information Sharing Around Elections Risk (CISA, DNI, FBI)
    - i. USG asking for specific questions to shape the brief.
    - b. Elections and Potential Impacts of U.S. Sanctions Against Russia (DNI/All)
3. Industry Meeting Topics (Facilitator: Meta)
  - a. *Proposed:* Status of full list of company best practices for elections officials on physical security as suggested in January call.
  - b. *Proposed:* How might punitive measures against Russia impact Industry's "risk calculus" vis-à-vis elections
    - i. USG is keen to hear specific info from industry on how actions against Russia might change their risk calculus; to the extent that any actions against Russia become elections issues in the U.S.

Lauren Protentis (She/Her)

Mis, Dis, and Mal-information (MDM) Team

Election Security Initiative

National Risk Management Center

Cybersecurity and Infrastructure Security Agency

O: [REDACTED] | Email: [REDACTED]@cisa.dhs.gov | HSDN: [REDACTED]@dhs.sgov.gov | CLAN: [REDACTED]@dhs.ic.gov



-----Original Appointment-----

**From:** [REDACTED]@fb.com>

**Sent:** Wednesday, January 12, 2022 4:19 PM

**To:** [REDACTED] Snell, Allison; Hale, Geoffrey; PROTENTIS, LAUREN; Schaul, Robert; SENNINGER, MARCUS; WYMAN, KIM; [REDACTED]

**Subject:** [PREP] USG | Industry Call (Bi-Monthly)

**When:** Wednesday, March 9, 2022 2:00 PM-2:30 PM (UTC-05:00) Eastern Time (US & Canada).

**Where:** [REDACTED]

**CAUTION:** This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

\*Prep Mtg - occurs the second Wednesday of every 2 months

\*Dial in updated 1/12<sup>th</sup>

Join Zoom Meeting

[REDACTED]

Meeting ID: 9 [REDACTED]

Passcode: [REDACTED]

One tap mobile

- + [REDACTED] US (Washington DC)
- + [REDACTED] US (New York)

**From:** Protentis, Lauren [/O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=604C2D8C37944283805D4BD9A9A83476-LAUREN.PROT]  
**Sent:** 7/20/2022 10:16:12 AM  
**To:** [REDACTED]@fb.com]; [REDACTED]@fb.com]; [REDACTED]@fb.com]  
**CC:** [REDACTED]@fb.com]  
**Subject:** Agenda: USG | Industry Call

Hi All,

Looking forward to connecting today, I pulled the agenda together below for today's call. Let me know if you have any questions.

1. Opening (Facilitator: Lauren)
2. Government Meeting Topics (Facilitator: Lauren)
- b. Information Sharing Around Elections Risk

i. **Annotation – Industry Prompts:**

1. (1) Races/states that you anticipate may be particularly targeted; (2) Themes/narratives/approaches you anticipate for races that you think will be targeted; (3) Specific indicators about infrastructure that foreign actors could use to target US; (4) Specific dates/events within the electoral calendar that you anticipate may be targeted; (5) May still be too early for this, but on inter-related risk between Ukraine and the US: does the developing situation increase (or decrease?) the risk that Russia may target the midterms?

ii. **Annotation – Briefing Structure**

4. CISA – Elections Infrastructure Risks (Scully)
5. DHS I&A – Infrastructure Activity (Beckman)
6. FBI – Domestic Adversarial Actor Update (Dehmlow)
7. DNI – Geopolitical Considerations ([REDACTED])
3. Industry Meeting Topics (Facilitator: Meta)

- a. Industry Briefs

i. **Annotation – USG Prompts:**

i. To what extent have you identified notable commonalities/differences between how foreign actors seek to use social media to influence their expatriate populations within the US on elections/other topics of strategic interest versus the broader US public? What stands out?

ii. Do you and to what extent assess that foreign actors display greater willingness to directly engage US political entities, US activists, and US media organizations that fall within diaspora communities? Do these engagements stand out to you or do you judge them as largely consistent with steady state foreign influence behavior across target audiences?

iii. To what extent or degree do you assess that PRC-linked or pro-CCP online influencers are amplifying divisive social and political issues in the United States?

Lauren Protentis (She/Her)  
 Mis, Dis, and Mal-information (MDM) Team  
 Election Security Initiative  
 National Risk Management Center  
 Cybersecurity and Infrastructure Security Agency

O: [REDACTED] | Email: [REDACTED]@cisa.dhs.gov | HSDN: [REDACTED]@dhs.sgov.gov | CLAN: [REDACTED]@dhs.ic.gov



**From:** Protentis, Lauren  
**Sent:** Friday, June 10, 2022 5:03 PM  
**To:** [REDACTED]@fb.com>; [REDACTED]@fb.com> [REDACTED]@fb.com>  
**Cc:** [REDACTED]@fb.com>  
**Subject:** RE: Rescheduled: [Prep] USG | Industry Call

Hi [REDACTED]

Thanks for the call yesterday. The USG passed along one additional question for you/industry to consider for your brief next week. Have a great weekend in VT!

- To what extent or degree do you assess that PRC-linked or pro-CCP online influencers are amplifying divisive social and political issues in the United States?

Lauren Protentis (She/Her)  
Mis, Dis, and Mal-information (MDM) Team  
Election Security Initiative  
National Risk Management Center  
Cybersecurity and Infrastructure Security Agency  
O: [REDACTED] | Email: [REDACTED]@cisa.dhs.gov | HSDN: [REDACTED]@dhs.sgov.gov | CLAN: [REDACTED]@dhs.ic.gov



-----Original Appointment-----

**From:** [REDACTED]@fb.com>  
**Sent:** Wednesday, June 8, 2022 2:46 PM  
**To:** [REDACTED]; Protentis, Lauren; Schaul, Robert; Senninger, Marcus; Wyman, Kim (She/Her/Hers); Hale, Geoffrey (He/Him); Snell, Allison (She/Her); Scully, Brian; [REDACTED]  
**Cc:** [REDACTED]  
**Subject:** Rescheduled: [Prep] USG | Industry Call  
**When:** Thursday, June 9, 2022 8:00 AM-8:30 AM (UTC-08:00) Pacific Time (US & Canada).  
**Where:** https://[REDACTED]

**CAUTION:** This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

WAYS TO JOIN

Join Zoom Meeting

[REDACTED]

Meeting ID: [REDACTED]  
Passcode: [REDACTED]

Computer or mobile guest sharable join link

[REDACTED]

One tap Mobile

+ [REDACTED] # US (San Jose)  
+ [REDACTED] # US (San Jose)

Dial by your location

toll: [REDACTED] San Jose US)  
toll: [REDACTED] (oma US)  
toll: [REDACTED] (uston US)  
toll: [REDACTED] (ashington DC US)  
toll: [REDACTED] (icago US)  
toll: [REDACTED] (w York US)  
toll: [REDACTED] (US)  
toll: [REDACTED] (US)  
toll: [REDACTED] (US)  
toll: [REDACTED] (US)  
Me [REDACTED] 4

Passcode: [REDACTED]

Join by SIP:

[REDACTED]

---

**From:** [REDACTED]@fb.com]  
**Sent:** 7/13/2020 6:17:20 AM  
**To:** Masterson, Matthew [REDACTED]@cisa.dhs.gov]  
**CC:** Scully, Brian [REDACTED]@cisa.dhs.gov]; [REDACTED]@fb.com]  
**Subject:** Re: Next Synch

Many thanks, Matt.

Appreciate the info/update. We'll lock in the date/time.

Let us know if we need to connect about the agenda in advance of Wednesday.

Best,  
Sandy

Sent from my iPhone

On Jul 10, 2020, at 4:18 PM, Masterson, Matthew <Matthew.Masterson@cisa.dhs.gov> wrote:

Sandy,

Lock in the date and time. We have not heard back on agenda from other feds so we will report back.

Thanks for your patience.

Matt

Matthew V. Masterson  
Senior Cybersecurity Advisor  
Department of Homeland Security  
Cybersecurity & Infrastructure Security Agency (CISA)  
[REDACTED]  
[REDACTED]@cisa.dhs.gov

---

**From:** [REDACTED]@fb.com>  
**Sent:** Friday, July 10, 2020 4:14:38 PM  
**To:** Masterson, Matthew <[REDACTED]@cisa.dhs.gov>; Scully, Brian [REDACTED]@cisa.dhs.gov>  
**Cc:** [REDACTED]@fb.com>  
**Subject:** Re: Next Synch

Gents,

Any update? We have a call at 4:30 today and would like to share any feedback you have.

Thanks!

[REDACTED]  
Sent from my iPhone

On Jul 9, 2020, at 6:54 AM, [REDACTED]@fb.com> wrote:

Good morning, Gents!

Wanted to share we have a synch with our industry peers tomorrow.

Would be helpful to have any feedback on agenda and if we can lock our next meeting for 2:00-3:30 pm EST next Wednesday, July 15th.

Thanks,  
[REDACTED]

Sent from my iPhone

On Jul 6, 2020, at 10:41 AM, [REDACTED]@fb.com> wrote:

Gents,

I hope you had a safe and happy Independence Day!

I wanted to follow-up on pushing our monthly synch out to next Wednesday (July 15th; same time 2:00-3:30 EST) and also get your feedback on the agenda proposed below.

Thoughts??  
[REDACTED]

Sent from my iPhone

On Jul 1, 2020, at 4:50 PM, [REDACTED]@fb.com> wrote:

Matt and Brian,

Thank you so much for the outreach on our next sync. Given the holiday weekend and various schedules, we were wondering if we could move our next meeting to Wednesday, July 15.

Below is a proposed agenda –please share your thoughts & feedback:

1. 10 minutes: Dial In/Opening
2. 30 minutes: Threat Updates
  1. Threat update from USG (FBI, I&A)
  2. Threat update from industry (FB, TW, GOOG)
3. 40 minutes: Deep Dive Topics (Industry/USG Moderated Discussion)
  1. Election process update from USG
  2. Hack/Leak and USG Attribution Speed/Process
  3. Vote-by-mail: How do we deal with the gap between Nov 3 and results?
4. 10 minutes: Highlights & Upcoming Watch Outs & Wrap (Moderated)?

Separately, on the GEC, we talked it over with our colleagues in industry and the feedback we received was that they would prefer to not add new participants at this time.



As always, happy to connect and walk through this.

Best for happy & safe 4<sup>th</sup> of July-

██████████

**From:** Scully, Brian [/O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=7CA10604AEE04B1DAB53DC9F884130BD-SCULLY, BRI]  
**Sent:** 6/17/2020 4:34:25 PM  
**To:** [REDACTED]@fb.com]; Masterson, Matthew [REDACTED]@cisa.dhs.gov]  
**CC:** [REDACTED]@fb.com]; [REDACTED]@fb.com]; [REDACTED]@fb.com]; Hale, Geoffrey [REDACTED]@cisa.dhs.gov]; Snell, Allison [REDACTED]@cisa.dhs.gov]; [REDACTED]@fb.com]; [REDACTED]@fb.com]  
**Subject:** RE: Call with NASS/NASED

As an FYI, Eva is cutting in and out a bit.

Brian

**From:** [REDACTED]@fb.com>  
**Sent:** Wednesday, June 17, 2020 4:32 PM  
**To:** Masterson, Matthew [REDACTED]@cisa.dhs.gov>  
**Cc:** Scully, Brian [REDACTED]@cisa.dhs.gov>; [REDACTED]@fb.com>; [REDACTED]@fb.com>; [REDACTED]@fb.com>; Hale, Geoffrey [REDACTED]@cisa.dhs.gov>; Snell, Allison [REDACTED]@cisa.dhs.gov>; [REDACTED]@fb.com>; [REDACTED]@fb.com>  
**Subject:** Re: Call with NASS/NASED

**CAUTION:** This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Yes. [REDACTED] will

I am running late

Sent from my iPhone

On Jun 17, 2020, at 4:31 PM, Masterson, Matthew [REDACTED]@cisa.dhs.gov> wrote:

Facebook friends I assume you are kicking this call off?

Matthew V. Masterson  
 Senior Cybersecurity Advisor  
 Department of Homeland Security  
 Cybersecurity & Infrastructure Security Agency (CISA)  
 [REDACTED]  
 [REDACTED]@hq.dhs.gov

**From:** [REDACTED]@fb.com>  
**Sent:** Tuesday, June 16, 2020 9:28 AM  
**To:** Scully, Brian [REDACTED]@cisa.dhs.gov>; Masterson, Matthew [REDACTED]@cisa.dhs.gov>  
**Cc:** [REDACTED]@fb.com>; [REDACTED]@fb.com>; [REDACTED]@fb.com>; Hale,

Geoffrey <[REDACTED]@cisa.dhs.gov>; Snell, Allison <[REDACTED]@cisa.dhs.gov> <[REDACTED]@fb.com>; <[REDACTED]@fb.com>

**Subject:** Re: Call with NASS/NASED

**CAUTION:** This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Good morning!

Fine to extend the invites to others. The bandwidth for the call should be sufficient.

Also, we don't have any docs to circulate in advance (at this point). That said, I do anticipate we could discuss items where we will follow up with info/docs.

Thanks again for your help facilitating the call!

Best,

---

**From:** "[REDACTED]@cisa.dhs.gov" <[REDACTED]@cisa.dhs.gov>

**Date:** Monday, June 15, 2020 at 1:55 PM

**To:** <[REDACTED]@fb.com>, <[REDACTED]@fb.com>

**Cc:** "Scully, Brian" <[REDACTED]@cisa.dhs.gov>, <[REDACTED]@fb.com>, <[REDACTED]@fb.com>

<[REDACTED]@fb.com>, <[REDACTED]@fb.com>, "[REDACTED]@cisa.dhs.gov"

<[REDACTED]@cisa.dhs.gov>, <[REDACTED]@cisa.dhs.gov" <[REDACTED]@cisa.dhs.gov>, <[REDACTED]@fb.com>

<[REDACTED]@fb.com>

**Subject:** RE: Call with NASS/NASED

Facebook Team,

I want to thank you for your willingness to brief the state and local officials this week. A couple questions:

- 1) Traditionally we have invited the entire GCC (state and local election official body we work most closely with) and the SCC Executive Committee (private sector leadership we work most closely with) to these calls. Is that ok?
- 2) Do you have any materials you want distributed in advance? No problem if not but wanted to make sure to ask.

Thanks.

Matt

Matthew V. Masterson  
Senior Cybersecurity Advisor  
Department of Homeland Security  
Cybersecurity & Infrastructure Security Agency (CISA)

<[REDACTED]@hq.dhs.gov>

**From:** [REDACTED]@fb.com>  
**Sent:** Wednesday, June 3, 2020 12:52 PM  
**To:** Masterson, Matthew [REDACTED]@cisa.dhs.gov>; [REDACTED]@fb.com>  
**Cc:** Scully, Brian [REDACTED]@cisa.dhs.gov>; [REDACTED]@fb.com>; [REDACTED]@fb.com>; [REDACTED]@fb.com>; Hale, Geoffrey [REDACTED]@cisa.dhs.gov>; Snell, Allison [REDACTED]@cisa.dhs.gov>; [REDACTED]@fb.com>  
**Subject:** RE: Call with NASS/NA SED

**CAUTION:** This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Hi All-

You should be receiving a calendar invite with the below dial-in details for the call on Wednesday, June 17 at 4:30p ET.

Best,

### Ways to join

🌐 Computer or Mobile:

[https://fb\\_workplace.com/meet/aFRKndg7rx/](https://fb_workplace.com/meet/aFRKndg7rx/)

☎ Telephone:

Dial in on [REDACTED] or find [an alternative number](#) then enter [REDACTED]

Enabled by OneVC

**From:** Masterson, Matthew [REDACTED]@cisa.dhs.gov>  
**Sent:** Tuesday, June 2, 2020 8:09 AM  
**To:** [REDACTED]@fb.com>  
**Cc:** Scully, Brian [REDACTED]@cisa.dhs.gov>; [REDACTED]@fb.com>; [REDACTED]@fb.com>; [REDACTED]@fb.com>; Hale, Geoffrey [REDACTED]@cisa.dhs.gov>; Snell, Allison [REDACTED]@cisa.dhs.gov>; [REDACTED]@fb.com>; [REDACTED]@fb.com>  
**Subject:** RE: Call with NASS/NA SED

Thanks [REDACTED] we will work with Becky. I would anticipate approx. 75-100 participants.

Matthew V. Masterson  
 Senior Cybersecurity Advisor  
 Department of Homeland Security  
 Cybersecurity & Infrastructure Security Agency (CISA)

[REDACTED]

From: [REDACTED]@fb.com>  
Sent: Tuesday, June 2, 2020 8:03 AM  
To: Masterson, Matthew <[REDACTED]@cisa.dhs.gov>  
Cc: Scully, Brian <[REDACTED]@cisa.dhs.gov>; [REDACTED]@fb.com>; [REDACTED]@fb.com>; [REDACTED]@fb.com>; Hale, Geoffrey <[REDACTED]@cisa.dhs.gov>; Snell, Allison <[REDACTED]@cisa.dhs.gov>; [REDACTED]@fb.com>; [REDACTED]@fb.com>  
Subject: Re: Call with NASS/NASED

**CAUTION:** This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Many thanks!

Including [REDACTED] to lock schedules for our team.

Also—please work with [REDACTED] on dial in. Happy to do a BJN or you can do a webex. We should use the platform that can best handle the volume (should we expect 60-70 people max for dial in? We had about 40 for our call with the State AG's in March). Whatever is best, is fine with me.

Thanks!!

Sent from my iPhone

On Jun 2, 2020, at 7:54 AM, Masterson, Matthew <[REDACTED]@cisa.dhs.gov> wrote:

[REDACTED]  
We have talked with NASS and NASED and they are comfortable with moving forward with a call. They requested **4:30 pm EST Wed, 17 Jun.**

The overall agenda and run of show looks good to us. The one item they noted that is of most interest is ongoing activity that you all are seeing and responding to. Particularly any insights you all have regarding disinformation regarding COVID and the recent protests even if there is no direct nexus to elections.

Matt

Matthew V. Masterson  
Senior Cybersecurity Advisor  
Department of Homeland Security  
Cybersecurity & Infrastructure Security Agency (CISA)  
[REDACTED]@hq.dhs.gov

From: [REDACTED]@fb.com>  
 Sent: Sunday, May 31, 2020 11:14 AM  
 To: Scully, Brian [REDACTED]@cisa.dhs.gov>; Masterson, Matthew [REDACTED]@cisa.dhs.gov>  
 Cc: [REDACTED]@fb.com>; [REDACTED]@fb.com>; [REDACTED]@fb.com>  
 Subject: Call with NASS/NASED

**CAUTION:** This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Brian & Matt,

It was great to connect last week.

Apologize for the weekend email, but I wanted to send this so you would have some time to think about it.

We would like to schedule a thirty minute call with NASS & NASED reps in the next few weeks and seek your assistance in helping coordinate the briefing.

Provided below is our proposed schedule & run of show. **On timing, we propose 4:30 pm EST Wed, 17 Jun or 3:00 pm EST Thurs, 18 Jun.** Do these dates/times work for you?

We can discuss dial-in instructions once we get closer.

Please let me know if you have any questions!

Thanks,  
 Sandy

**Expected Attendees:**

- NASS & NASED Leads or their designated representatives.

**Additional Invitees:**

- DHS. Representatives from CISA/Countering Foreign Influence Task Force  
 - FBI Representatives from the FBI Foreign Influence Task Force

**Moderators:**

[REDACTED] Director of Public Policy  
 [REDACTED] Public Policy Manager

**FB Briefers:**

-Overview of Security Policy & Election Integrity Efforts ([REDACTED])  
 -Overview of our efforts to address Coordinated Inauthentic Behavior (CIB) ([REDACTED])  
 -Overview of our work with Law Enforcement/FBI ([REDACTED])  
 -Overview of our Election Misinformation Policy & Reporting Structure ([REDACTED])

**Run of Show:**

Open call; Welcome  
 Brief Comments by DHS & FBI  
 Introduction of FB briefers  
 Facebook briefing  
 Q&A

Briefing complete

From: [redacted]@fb.com]
Sent: 4/13/2022 1:02:19 PM
To: Protentis, Lauren [redacted]@cisa.dhs.gov]; [redacted]@fb.com]; [redacted]@fb.com]; [redacted]@fb.com]
CC: [redacted]@fb.com]
Subject: RE: Calendar Invite Updates - Monthly Meetings

Thank you so much – the invite has been updated.

[redacted]



[redacted] (she/her/hers)
Executive Business Partner | Trust & Safety Policy

From: Protentis, Lauren <[redacted]@cisa.dhs.gov>
Sent: Wednesday, April 13, 2022 8:32 AM
To: [redacted]@fb.com>; [redacted]@fb.com>; [redacted]@fb.com>; [redacted]@fb.com>
Cc: [redacted]@fb.com>
Subject: RE: Calendar Invite Updates - Monthly Meetings

Hi [redacted], How about 1:00-1:30 tomorrow? Sorry for the delay.

Lauren Protentis (She/Her)
Mis, Dis, and Mal-information (MDM) Team
Election Security Initiative
National Risk Management Center
Cybersecurity and Infrastructure Security Agency
O: [redacted] | Email: [redacted]@cisa.dhs.gov | HSDN: [redacted]@dhs.gov | CLAN: [redacted]@dhs.ic.gov



From: [redacted]@fb.com>
Sent: Tuesday, April 12, 2022 3:13 PM
To: Protentis, Lauren [redacted]@cisa.dhs.gov>; [redacted]@fb.com>; [redacted]@fb.com>; [redacted]@fb.com>
Cc: [redacted]@fb.com>; [redacted]@fb.com>
Subject: Re: Calendar Invite Updates - Monthly Meetings

Good Afternoon Lauren,

Apologies for the thrash on this but unfortunately Thursday at 2pm ET will not work on our end. Can your group do any of the below times on Thursday, 04/14?

12pm - 130pm ET or 4pm - 5pm ET

Again, apologies for the back & forth on this one.



██████████  
Sent from my Verizon, Samsung Galaxy smartphone  
Get [Outlook for Android](#)

---

**From:** Protentis, Lauren <██████████@cisa.dhs.gov>  
**Sent:** Sunday, April 3, 2022 1:57:02 PM  
**To:** ██████████@fb.com>; ██████████@fb.com>; ██████████@fb.com>; ██████████@fb.com>  
**Cc:** ██████████@fb.com>; ██████████@fb.com>  
**Subject:** Re: Calendar Invite Updates - Monthly Meetings

Hi ██████████, thank you. 4/14 at 2:00 for the prep call works well for us. Confirming we can lock in that time for the prep call.

**Lauren Protentis • Mis, Dis, Malinformation Team • National Risk Management Center • Cybersecurity and Infrastructure Security Agency (CISA)**

M: ██████████ E: ██████████@cisa.dhs.gov | HSDN: ██████████@dhs.gov |  
CLAN: ██████████@dhs.gov

---

**From:** ██████████@fb.com>  
**Sent:** Friday, April 1, 2022 4:23:12 PM  
**To:** ██████████@cisa.dhs.gov>; ██████████@fb.com>; ██████████@fb.com>; ██████████@fb.com>  
**Cc:** ██████████@fb.com>; ██████████@fb.com>  
**Subject:** RE: Calendar Invite Updates - Monthly Meetings

Hi Lauren,

The USG | Industry invite is updated.

For the prep, we still run into the same flag that ██████████ will be in flight on 04/13 – it sounds like your team isn't available on 04/14 at 2pm ET either. Would you like to propose other times for this one-off prep on 04/14 or 04/15? I can take your options back to Meta and Industry and we can land it from there.

Thank you,

---

**From:** Protentis, Lauren <██████████@cisa.dhs.gov>  
**Sent:** Thursday, March 31, 2022 5:56 AM  
**To:** ██████████@fb.com>; ██████████@fb.com>; ██████████@fb.com>; ██████████@fb.com>  
**Cc:** ██████████@fb.com>  
**Subject:** RE: Calendar Invite Updates - Monthly Meetings

Hi ██████████, If it's okay with your side, we'd like to go stick with the weeks 2 and 3. It's been an ongoing challenge to get a date that works for everyone and that's the preference for the USG. Thanks so much!

Lauren Protentis (She/Her)  
Mis, Dis, and Mal-information (MDM) Team  
Election Security Initiative  
National Risk Management Center  
Cybersecurity and Infrastructure Security Agency  
O: [REDACTED] | Email: [REDACTED]@cisa.dhs.gov | HSDN: [REDACTED]@dhs.sgov.gov | CLAN:  
[REDACTED]@dhs.ic.gov



From: [REDACTED]@fb.com>  
Sent: Wednesday, March 30, 2022 3:38 PM  
To: Protentis, Lauren <[REDACTED]@cisa.dhs.gov>; [REDACTED]@fb.com> [REDACTED]  
[REDACTED]@fb.com>; [REDACTED]@fb.com>  
Cc: [REDACTED]@fb.com>; [REDACTED]@fb.com>  
Subject: RE: Calendar Invite Updates - Monthly Meetings

Hi Lauren,

Yes, I did catch this. I synced with Nathaniel who agreed with your recommendation to have the prep on week 1 and full call on week 2. However, if it doesn't work for your team, we can shift the mtgs back to weeks 2 and 3.

[REDACTED]

From: Protentis, Lauren [REDACTED]@cisa.dhs.gov>  
Sent: Wednesday, March 30, 2022 6:19 AM  
To: [REDACTED]@fb.com>; [REDACTED]@fb.com>; [REDACTED]@fb.com>;  
[REDACTED]@fb.com>  
Cc: [REDACTED]@fb.com>  
Subject: RE: Calendar Invite Updates - Monthly Meetings

Hi [REDACTED], After this exchange, I realized the calendar cadence moved to the 2<sup>nd</sup> Wednesday of the month, when we had been meeting the 3<sup>rd</sup> Wednesday of every month. So, I think our next meeting should be April 20<sup>th</sup>, vice April 14<sup>th</sup>. And the following meeting would be May 18<sup>th</sup>. The 3<sup>rd</sup> Wednesday cadence works best for our side.

Can you modify on your end?

Let me know if you have any questions/concerns!

Lauren Protentis (She/Her)  
Mis, Dis, and Mal-information (MDM) Team  
Election Security Initiative  
National Risk Management Center  
Cybersecurity and Infrastructure Security Agency  
O: [REDACTED] | Email: [REDACTED]@cisa.dhs.gov | HSDN: [REDACTED]@dhs.sgov.gov | CLAN:  
[REDACTED]@dhs.ic.gov



**From:** [REDACTED]@fb.com>  
**Sent:** Monday, March 28, 2022 2:46 PM  
**To:** Protentis, Lauren [REDACTED]@cisa.dhs.gov>; [REDACTED]@fb.com>; [REDACTED]@fb.com>; [REDACTED]@fb.com>  
**Cc:** [REDACTED]@fb.com>; [REDACTED]@fb.com>  
**Subject:** RE: Calendar Invite Updates - Monthly Meetings

**CAUTION:** This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Hi Lauren,

Happy Monday!! I'm happy to update the invites accordingly – one quick flag that Nathaniel will be on a flight on 04/13. Can your team meet at the same time, 2pm ET, on Thursday, 04/14? Please confirm and I'll send the updated invites.

Thank you,

Sarina

**From:** Protentis, Lauren [REDACTED]@cisa.dhs.gov>  
**Sent:** Thursday, March 24, 2022 6:26 AM  
**To:** [REDACTED]@fb.com>; [REDACTED]@fb.com>; [REDACTED]@fb.com>  
**Cc:** [REDACTED]@fb.com>; [REDACTED]@fb.com>  
**Subject:** Calendar Invite Updates - Monthly Meetings

Hi All, Thanks for the call yesterday – we'll follow-up shortly with some due-outs.

Logistically, we'll need the invite (which Meta manages) to be updated to a monthly meeting cadence and our pre -syncs to follow suit. Would you kindly send us updated invites and Kim Wyman ([REDACTED]@cisa.dhs.gov)? According to the cal, our next meeting would be April 13<sup>th</sup>; the pre-sync April 6<sup>th</sup>.

Let me know if you have any questions and thanks so much!

Lauren Protentis (She/Her)  
Mis, Dis, and Mal-information (MDM) Team  
Election Security Initiative  
National Risk Management Center  
Cybersecurity and Infrastructure Security Agency  
O: [REDACTED] | Email: [REDACTED]@cisa.dhs.gov | HSDN: [REDACTED]@dhs.sgov.gov | CLAN:  
[REDACTED]@dhs.ic.gov



From: [REDACTED]@twitter.com]  
Sent: 1/11/2021 7:53:03 PM  
To: Scully, Brian [REDACTED]@cisa.dhs.gov]  
Subject: Re: Threat Brief

**CAUTION:** This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Hi Brian, sorry for my delay in responding.

We will prioritize scheduling the briefing and try to accommodate your schedule. Do you and the team have availability on Thursday afternoon?

We had temporary clearances for the 30 around the election, but I believe they have expired. Do the briefest think we can have a meaningful conversation on the unclassified side? (Might also be difficult to conduct since we are all remote.)

Please connect me to the ODNI NCSC — thank you!

We are eager to receive a briefing on any topics that might be relevant to Twitter or the conversation last that might occur on the platform. I will send you some of the information we have removed for your awareness a little later tonight.

Thanks so much, I really appreciate all your assistance today and throughout the election season.

Thanks,  
[REDACTED]

On Mon, Jan 11, 2021 at 7:41 PM Scully, Brian <[REDACTED]@cisa.dhs.gov> wrote:

Hi [REDACTED],

Wanted to see if you had some time slots available for the threat brief I could pass to I&A?

On a separate note, I had a colleague at ODNI's NCSC (Counterintelligence office) ask to be connected with you all. Any issue with me providing an email introduction?

Thanks,  
Brian

**From:** [REDACTED]@twitter.com]  
**Sent:** 4/13/2020 10:35:29 AM  
**To:** Scully, Brian [REDACTED]@cisa.dhs.gov]  
**CC:** Masterson, Matthew [REDACTED]@cisa.dhs.gov]  
**Subject:** Re: Gov't/Industry Meeting

**CAUTION:** This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Thank you for letting me know.

On Mon, Apr 13, 2020 at 10:28 AM Scully, Brian <[REDACTED]@cisa.dhs.gov> wrote:  
Stacia,

As an FYI, we have been told the Acting DNI will not join the call on Thursday. Hopefully that makes things easier for everyone.

Regards,  
Brian

---

**From:** [REDACTED]@twitter.com>  
**Sent:** Friday, April 10, 2020 6:53 PM  
**To:** Scully, Brian [REDACTED]@cisa.dhs.gov>  
**Cc:** Masterson, Matthew [REDACTED]@cisa.dhs.gov>  
**Subject:** Re: Gov't/Industry Meeting

**CAUTION:** This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Thanks so much for letting us know. I think that will impact the level of staff (probably need to loop in VPs) we have on the call if Acting Director Grenell is on the call so I will start preparing for that possibility.

On Fri, Apr 10, 2020 at 5:18 PM Scully, Brian <[REDACTED]@cisa.dhs.gov> wrote:  
Stacia,

One additional note. It is possible the Acting Director National Intelligence will participate on the call. We've requested he only participate by providing welcome/intro comments, but it's possible he'll remain on the call for longer. I'll keep you posted.

Brian

**From:** [REDACTED]@twitter.com>  
**Sent:** Friday, April 10, 2020 3:58 PM  
**To:** Scully, Brian [REDACTED]@cisa.dhs.gov>  
**Cc:** Masterson, Matthew [REDACTED]@cisa.dhs.gov>  
**Subject:** Re: Gov't/Industry Meeting

**CAUTION:** This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Do you have a sense of the government side attendees?

On Fri, Apr 10, 2020 at 2:54 PM [REDACTED]@twitter.com> wrote:  
Hi Brian, is it the weekend yet?

I spoke to Yoel. He estimates approximately 30 industry attendees -- but he believes that could be higher or lower depending on how the remote meeting affects things. Companies which have attended in the past include: Twitter, Facebook (including other Facebook properties), Google (including other Alphabet properties), Verizon Media, Microsoft, LinkedIn, and Reddit. Possible additions include Medium and Pinterest.

Yoel said the agenda looks good.

Let me know if you need anything else.

[REDACTED]

On Fri, Apr 10, 2020 at 9:50 AM Scully, Brian [REDACTED]@cisa.dhs.gov> wrote:

Thanks [REDACTED] One additional question while I have you – do you have a number of participants on the industry side? I may need a rough estimate for setting up the VTC. Also, would be good to know which companies will be participating.

Brian

**From:** [REDACTED]@twitter.com>  
**Sent:** Friday, April 10, 2020 9:47 AM  
**To:** Scully, Brian [REDACTED]@cisa.dhs.gov>  
**Cc:** Masterson, Matthew [REDACTED]@cisa.dhs.gov>  
**Subject:** Re: Gov't/Industry Meeting

**CAUTION:** This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Will forward onto SF and let you know what I hear.

Thank you!

On Fri, Apr 10, 2020 at 9:28 AM Scully, Brian <[REDACTED]@cisa.dhs.gov> wrote:

Hi [REDACTED]

ODNI is unable to use Microsoft Teams, so we're looking to use Cisco WebX for the VTC. Let me know if there are any issues.

Also, please see the attached draft agenda. Let me know if you all have any changes.

Thanks,

Brian

---

**From:** [REDACTED]@twitter.com>  
**Sent:** Wednesday, April 8, 2020 11:03 AM  
**To:** Scully, Brian [REDACTED]@cisa.dhs.gov>  
**Cc:** Masterson, Matthew [REDACTED]@cisa.dhs.gov>  
**Subject:** Re: Govt/Industry Meeting

**CAUTION:** This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Let's plan on April 16th at 2pm EST. No industry peers have raised any blockers.

If you can set it up through Microsoft Teams, that would be excellent and much appreciated.

Thank you,

On Mon, Apr 6, 2020 at 8:44 AM [REDACTED]@twitter.com> wrote:

Thank you, Brian. Let me send this date to the folks in SF.

I will also ensure industry peers can handle Teams. Our CorpSec told us last week we are not allowed to use Zoom.

Thank you for your help!

On Mon, Apr 6, 2020 at 8:43 AM Scully, Brian <[REDACTED]@cisa.dhs.gov> wrote:

Hi [REDACTED]

Can we schedule the meeting for Thursday, April 16<sup>th</sup> at 2pm EST? I'll put together a more formal agenda and send around. How would you all like to handle the video call? I can set something up through Microsoft Teams unless you all prefer a different tool.

Thanks,

Brian

**From:** [REDACTED]@twitter.com>  
**Sent:** Tuesday, March 31, 2020 4:12 PM  
**To:** Scully, Brian <[REDACTED]@cisa.dhs.gov>  
**Cc:** Masterson, Matthew <[REDACTED]@cisa.dhs.gov>  
**Subject:** Re: Gov't/Industry Meeting

**CAUTION:** This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Everyone was in agreement that 90 minutes max made sense. No objections to the agenda, and I think it makes sense to tie in COVID disinformation since we saw that intersection in the Ohio primary in advance of the postponement.

On Tue, Mar 31, 2020 at 4:10 PM Scully, Brian <[REDACTED]@cisa.dhs.gov> wrote:

Thanks Stacia.

Did industry have thoughts on agenda or length of meeting? Want to see how much time we'll need.

Regards,

Brian

**From:** [REDACTED]@twitter.com>  
**Sent:** Tuesday, March 31, 2020 4:08 PM  
**To:** Scully, Brian <[REDACTED]@cisa.dhs.gov>  
**Cc:** Masterson, Matthew <[REDACTED]@cisa.dhs.gov>  
**Subject:** Re: Gov't/Industry Meeting

**CAUTION:** This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.



Hi Brian and Matthew, we coordinated on the industry side. There are no dates that the industry group cannot make, but there is a preference to do any day BUT Tuesdays. Please pick a date and time that works on your end (needs to be an afternoon to accommodate west coast) and let me know!

On Thu, Mar 26, 2020 at 5:02 PM [REDACTED]@twitter.com> wrote:

Thank you, Brian! You have the special status of my first work phone call completely derailed by my kids. But over the course of the last 10 days, you are certainly not my only!

Let me forward this onto folks in SF. They are coordinating with FB and others [REDACTED] at FB is pushing on scheduling this meeting) and I will come back to you with some feedback.

Thanks again, and talk soon Stay healthy!

[REDACTED]

On Thu, Mar 26, 2020 at 4:45 PM Scully, Brian [REDACTED]@cisa.dhs.gov> wrote:

Hey Stacia,

Hope you all are surviving week 2 ok. ☺ The Scully house is getting a bit testy at times, but otherwise doing fine.

Wanted to follow-up with you regarding a possible industry/government meeting. Based on interagency input, we're looking to do a video conference the second week of April. Please let me know if there are good/bad dates that week. From an agenda standpoint, we would suggest a shorter meeting, maybe 90 minutes, that covers a few specific topics. We're obviously flexible on length of meeting and agenda, but know everyone is a bit frenetic right now. Possible agenda items could include:

- What have we learned from the primaries so far, with a particular focus on Super Tuesday?
- With the changes to elections from Coronavirus, what do we expect for the rest of primary season and how will that translate to the General election in November?
- What activity are we seeing around Coronavirus generally?
- Other industry generated topics?

Happy to jump on a call if it would be helpful.

Thanks [REDACTED]

Brian

Brian Scully

Chief, Countering Foreign Influence Task Force  
DHS/CISA/NRMC



[REDACTED]@cisa.dhs.gov

[REDACTED]

**From:** Scully, Brian [/O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=7CA10604AEE04B1DAB53DC9F884130BD-SCULLY, BRI]  
**Sent:** 3/25/2020 12:17:14 PM  
**To:** [REDACTED]@fb.com]  
**Subject:** RE: Disinfo Campaign Targeting DS Officer

Thanks Saleela. Hope you and the family are also well.

Brian

**From:** [REDACTED]@fb.com>  
**Sent:** Wednesday, March 25, 2020 11:33 AM  
**To:** Scully, Brian [REDACTED]@cisa.dhs.gov>; [REDACTED]@fb.com>  
**Subject:** RE: Disinfo Campaign Targeting DS Officer

**CAUTION:** This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Thank you so much for this! Have flagged for our internal teams. As always, we really appreciate the outreach and sharing of this information. Hope you and your family are safe and sound!

**From:** Scully, Brian [REDACTED]@cisa.dhs.gov>  
**Sent:** Wednesday, March 25, 2020 11:05 AM  
**To:** [REDACTED]@fb.com>; [REDACTED]@fb.com>  
**Subject:** FW: Disinfo Campaign Targeting DS Officer

[REDACTED] and [REDACTED]

Please see the below reporting from our State Department Global Engagement Center colleagues about disinformation on YouTube targeting a Diplomatic Security Officer.

Regards,  
 Brian

*The U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) is not the originator of this information. CISA is forwarding this information, unedited, from its originating source – this information has not been originated or generated by CISA. This information may also be shared with law enforcement or intelligence agencies.*

*In the event that CISA follows up to request further information, such a request is not a requirement or demand. Responding to this request is voluntary and CISA will not take any action, favorable or unfavorable, based on decisions about whether or not to respond to this follow-up request for information.*

**From:** Dempsey, Alex L [REDACTED]@state.gov>  
**Sent:** Wednesday, March 25, 2020 10:30 AM  
**To:** Schaul, Robert  
**Subject:** Disinfo Campaign Targeting DS Officer



**CAUTION:** This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Rob,

Our leadership has asked that we share the below information with our IA counterparts. There is a disinfo campaign on Youtube targeting a DS Officer, claiming she brought COVID-19 to during an athletic competition. FYSA FBI has been alerted.

**Who: DS Officer, Maatje Benassi**

**What: Targeted Disinformation Campaign**

**When: O/A March 24<sup>th</sup>**

**Where: Online** [REDACTED]

**Why:**

Special Envoy, Lea Gabrielle received a note from a journalist on March 24<sup>th</sup> who tells me there is a false narrative being pushed online about someone who is believed to be a Diplomatic Security officer. Her name is Maatje Benassi. The journalist tells me there is a Youtube channel run by Americans falsely claiming she is "Patient Zero" and that as a U.S. Army reservist she brought COVID-19 to Wuhan during an athletic competition.

V/r,

Alex

**From:** [REDACTED]@fb.com]  
**Sent:** 3/13/2020 11:13:52 AM  
**To:** Scully, Brian [REDACTED]@cisa.dhs.gov]  
**CC:** [REDACTED]@fb.com]  
**Subject:** Re: Tweet regarding voting & COVID-19 - DISINFORMATION

**CAUTION:** This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Thanks, Brian!

Sent from my iPhone

On Mar 13, 2020, at 10:55 AM, Scully, Brian [REDACTED]@cisa.dhs.gov> wrote:

[REDACTED] and [REDACTED]

Apparently the tweet I sent has been taken down. Please see the screenshot below with the tweet.

Thanks,  
 Brian

**From:** Masterson, Matthew [REDACTED]@cisa.dhs.gov>  
**Sent:** Friday, March 13, 2020 10:51 AM  
**To:** Scully, Brian [REDACTED]@cisa.dhs.gov>  
**Cc:** Hale, Geoffrey [REDACTED]@cisa.dhs.gov>; Snell, Allison [REDACTED]@cisa.dhs.gov>  
**Subject:** FW: Tweet regarding voting & COVID-19 - DISINFORMATION

From OH in screen shot form and reported to CIOCC.

Matthew V. Masterson  
 Senior Cybersecurity Advisor  
 Department of Homeland Security  
 Cybersecurity & Infrastructure Security Agency (CISA)  
 [REDACTED]  
 [REDACTED]@hq.dhs.gov

**From:** Wood, Spencer [REDACTED]@OhioSOS.Gov>  
**Sent:** Friday, March 13, 2020 10:39 AM  
**To:** SecurityEvent <[REDACTED]@OhioSOS.Gov>; elections [REDACTED]@msisac.org>; MS-ISAC <[REDACTED]@msisac.org>  
**Cc:** Masterson, Matthew [REDACTED]@cisa.dhs.gov>; Keeling, Jon [REDACTED]@OhioSOS.Gov>; Grandjean, Amanda <[REDACTED]@OhioSOS.Gov>; Burns, [REDACTED]@OhioSOS.Gov>; Keeling, Jon <[REDACTED]@OhioSOS.Gov>; Shaffer, Grant <[REDACTED]@OhioSOS.Gov>; McAfee, Sean <[REDACTED]@OhioSOS.Gov>  
**Subject:** Tweet regarding voting & COVID-19 - DISINFORMATION

**CAUTION:** This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

The following disinformation regarding upcoming Ohio, Florida, Illinois, Louisiana, and Wisconsin elections and COVID-19 was posted to twitter:

<https://twitter.com/coocbie/status/1238465759745134593?s=21>

<image.png>

<~WRD318.jpg>

**Spencer Wood | Chief Information Officer**

Office of the Ohio Secretary of State

P: + [REDACTED] C: + [REDACTED]

[OhioSoS.gov](http://OhioSoS.gov)



# Thread



**Caden**  
@coocbie

DEAR ALL BOOMERS,

Due to COVID-19, it should be in your highest interest to refrain from entering polling stations in Illinois, Florida, Ohio, Louisiana, and Wisconsin!!!

This is for your own safety.

I repeat, BOOMERS DO NOT VOTE

10:03 AM · 3/13/20 · [Twitter Web App](#)

6 Likes



Caden @coocbie 25m

Tweet your reply



---

**From:** Masterson, Matthew [/O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=96EE6758666E4BD19924CB287A857503-MATTHEW.MAS]  
**Sent:** 6/2/2020 1:57:42 PM  
**To:** Scully, Brian [REDACTED]@cisa.dhs.gov]; [REDACTED]@twitter.com]  
**CC:** [REDACTED]@twitter.com]  
**Subject:** RE: Primary Election Day

[REDACTED]

Just to confirm what Brian said. Very quiet so far. Please let us know if any of the items passed to you today are worth understanding further or if something changes. Thanks

Matt

Matthew V. Masterson  
Senior Cybersecurity Advisor  
Department of Homeland Security  
Cybersecurity & Infrastructure Security Agency (CISA)  
[REDACTED]  
[REDACTED]@hq.dhs.gov

---

**From:** Scully, Brian [REDACTED]@cisa.dhs.gov>  
**Sent:** Tuesday, June 2, 2020 1:41 PM  
**To:** [REDACTED]@twitter.com>; Masterson, Matthew [REDACTED]@cisa.dhs.gov>  
**Cc:** [REDACTED]@twitter.com>  
**Subject:** RE: Primary Election Day

Hi [REDACTED]

It has been quiet on our end as well. As an FYI, we're expecting to receive some info from Colorado about fake accounts. Will send along once I get it.

Matt is on a call right now, so he may have more to add or a different perspective, but no issues on my end not doing a call.

Regards,  
Brian

---

**From:** [REDACTED]@twitter.com>  
**Sent:** Tuesday, June 2, 2020 1:37 PM  
**To:** Scully, Brian [REDACTED]@cisa.dhs.gov>; Masterson, Matthew [REDACTED]@cisa.dhs.gov>  
**Cc:** [REDACTED]@twitter.com>  
**Subject:** Re: Primary Election Day

**CAUTION:** This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.



Hi Matthew and Brian, we just wanted to check in.

We are tracking the curfew issues and have our legal team reviewing specificity-curfeews in the key primary states. Our enforcement teams are prepared on the issue.

We have received some escalations from external stakeholders, including the FBI.

Things seem generally quiet -- so if it works ok for you -- let's plan to not meet today. Please just let us know if anything comes up.

Stacia

On Mon, Jun 1, 2020 at 4:25 PM [REDACTED] <[\[REDACTED\]@twitter.com](#)> wrote:

Dear Matthew and Brian, hope you are well.

We are preparing for elections tomorrow. In case anything comes up urgently, please feel free to call me at [REDACTED] or reach us via email.

Should we plan to set up a mid-day check in? Does 2:30 work for you?

Thanks,  
[REDACTED]

---

**From:** Scully, Brian [/O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=7CA10604AEE04B1DAB53DC9F884130BD-SCULLY, BRI]  
**Sent:** 9/25/2020 11:31:16 AM  
**To:** [REDACTED]@twitter.com]  
**CC:** [REDACTED]@twitter.com]; Dragseth, John [REDACTED]@cisa.dhs.gov]  
**Subject:** RE: Election Disinfo Reporting

5pm today is fine. I'll send an invite.

---

**From:** [REDACTED]@twitter.com>  
**Sent:** Friday, September 25, 2020 11:30 AM  
**To:** Scully, Brian [REDACTED]@cisa.dhs.gov>  
**CC:** [REDACTED]@twitter.com>; Dragseth, John [REDACTED]@cisa.dhs.gov>  
**Subject:** Re: Election Disinfo Reporting

**CAUTION:** This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

That sounds great!. Is 5pm today or Monday ok?

On Fri, Sep 25, 2020 at 11:18 AM Scully, Brian <[REDACTED]@cisa.dhs.gov> wrote:

Good Morning Stacia and Lisa,

Do you all have 5 minutes for a quick call today? I'd like to give you a quick update on our reporting process this year. I'm free the rest of the day, so whenever works for you.

Thanks,

Brian

Brian Scully

Chief, Countering Foreign Influence Task Force

DHS/CISA/NRMC

[REDACTED]@cisa.dhs.gov

[REDACTED]

**From:** [REDACTED]@twitter.com]  
**Sent:** 9/10/2020 12:59:50 PM  
**To:** Masterson, Matthew [REDACTED]@cisa.dhs.gov]; Scully, Brian [REDACTED]@cisa.dhs.gov]  
**CC:** [REDACTED]@twitter.com]  
**Subject:** Update on Twitter's Civic Integrity Policy

**CAUTION:** This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Hi Matthew and Brian, hope you are both very well.

We want to give you an update. Today, we are updating our Civic Integrity Policy. Our existing Civic Integrity Policy targets the most directly harmful types of content, namely those related to:

- Information or false claims on how to participate in civic processes
- Content that could intimidate or suppress participation
- False affiliation

Starting next week, we will label or remove false or misleading information intended to undermine public confidence in an election or other civic process. This includes but is not limited to:

- False or misleading information that causes confusion about the laws and regulations of a civic process, or officials and institutions executing those civic processes
- Disputed claims that could undermine faith in the process itself, e.g. unverified information about election rigging, ballot tampering, vote tallying, or certification of election results
- Misleading claims about the results or outcome of a civic process which calls for or could lead to interference with the implementation of the results of the process, e.g. claiming victory before election results have been certified, inciting unlawful conduct to prevent a peaceful transfer of power or orderly succession

You can find additional information [here](#) and [here](#).

Thanks so much,  
[REDACTED]

**Sent:** 10/27/2020 4:25:44 PM  
**To:** [REDACTED]@twitter.com]; [REDACTED]@twitter.com]; [REDACTED]  
 [REDACTED]@twitter.com]  
**CC:** CFITF [REDACTED]@hq.dhs.gov]; [REDACTED]@cisecurity.org  
**Subject:** FW: Flagging Three Twitter Accounts Impersonating Colorado Government

Please see below report from Colorado. I've asked them if these accounts have already been reported, but these are screenshots from today.

Regards,  
 Brian

The Cybersecurity and Infrastructure Security Agency (CISA) of the U.S. Department of Homeland Security (DHS) is not the originator of this information. CISA is forwarding this information, unedited, from its originating source – this information has not been originated or generated by CISA. This information may also be shared with law enforcement or intelligence agencies.

CISA affirms that it neither has nor seeks the ability to remove or edit what information is made available on social media platforms. CISA makes no recommendations about how the information it is sharing should be handled or used by social media companies. Additionally, CISA will not take any action, favorable or unfavorable, toward social media companies based on decisions about how or whether to use this information.

**From:** Aaron Hayman <[REDACTED]@SOS.STATE.CO.US>  
**Sent:** Tuesday, October 27, 2020 4:17 PM  
**To:** [REDACTED]@cisecurity.org; Masterson, Matthew <[REDACTED]@cisa.dhs.gov>; Scully, Brian <[REDACTED]@cisa.dhs.gov>  
**Cc:** Trevor Timmons <[REDACTED]@SOS.STATE.CO.US>; Craig Buesing <[REDACTED]@SOS.STATE.CO.US>; Nathan Blumenthal <[REDACTED]@SOS.STATE.CO.US>; Josh Craven <[REDACTED]@SOS.STATE.CO.US>; Judd Choate <[REDACTED]@SOS.STATE.CO.US>; Hilary Rudy <[REDACTED]@SOS.STATE.CO.US>; Melissa Kessler <[REDACTED]@SOS.STATE.CO.US>; Ian Rayder <[REDACTED]@SOS.STATE.CO.US>; Betsy Hart <[REDACTED]@SOS.STATE.CO.US>; [REDACTED] <Steve.Hurlbert@SOS.STATE.CO.US>; Marygrace Galston <[REDACTED]@SOS.STATE.CO.US>; Grenis, Timothy <[REDACTED]@HQ.DHS.GOV>; Eastman - CDPS, Jerry <[REDACTED]@state.co.us>; Lisa Kaplan <[REDACTED]@aletheagroup.com>; Kristin Centanni <[REDACTED]@srg.com>; [REDACTED]@state.co.us; Bomba, Kristina <[REDACTED]@state.co.us>; Rhoads, Devon <[REDACTED]@state.co.us>; Rich Schliep <[REDACTED]@SOS.STATE.CO.US>  
**Subject:** Flagging Three Twitter Accounts Impersonating Colorado Government

**CAUTION:** This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

EI-ISAC and CISA Partners,

Three Twitter accounts (@c\_ogov, @OfficalColorado, @COstateGov) popped up in the last couple of weeks impersonating the Colorado state government. As you may be aware, numerous other similar accounts have also been created impersonating other state and city jurisdictions in recent weeks. The MS-ISAC flagged a couple of them last week (@c\_ogov//@officalColorado) but we don't know if the third one (@COstateGov) is on everyone's radar. Has anyone engaged Twitter about these? Welcome any additional information you have.

These are concerning to us here in Colorado because of the recent FBI/CISA warnings about impersonation accounts spreading false information about the election. For the Colorado accounts:

- All three joined Twitter this month – October 2020
- All three have a URL link prominently labeled “Colorado.gov” that takes users to the official Colorado.gov website after passing through several other systems that could be harvest data or be more nefarious.
- All follow/are followed by up to a couple dozen other state/local government impersonation accounts – many also created recently.
- Several look like they were temporarily suspended by Twitter but at least some appear to be back online.

Below are screenshots taken today of the three accounts:





**Colorado State Government**  
@COStateGov

Smoke weed erry day. The official (unofficial) Twitter account of the State of Colorado.

Colorado, USA [colorado.gov](https://colorado.gov) Joined October 2020

21 Following 27 Followers



**Not Actually Colorado**  
@OfficalColorado

The (UN)official Colorado Twitter Account. This is a parody account.

Colorado [colorado.gov](https://colorado.gov) Joined October 2020

12 Following 56 Followers

**Disclaimer:** Colorado Department of State is not the originator of the above information and is forwarding it, unedited, from its original source. The Department does not seek the ability to remove or edit what information is made available

on social media platforms. The Department makes no recommendations about how the information it is sharing should be handled or used by recipients of this email. The Department may also share this information with local, state, and federal government agencies.

**Aaron Hayman**  
Senior Elections Security Specialist  
(office)  
[@sos.state.co.us](mailto:hayman@sos.state.co.us)



From: [REDACTED]@fb.com]  
 Sent: 11/7/2020 5:00:52 AM  
 To: Masterson, Matthew [REDACTED]@cisa.dhs.gov]; Scully, Brian [REDACTED]@cisa.dhs.gov]  
 Subject: October CIB Report

**CAUTION:** This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Gents,

I hope you are well--what a week! Thank you for your continued partnership.

I also wanted to share that on November 6th we published our [October CIB report](#), including all networks we've taken down in the month of October which were engaged in [foreign or government interference](#) and [coordinated inauthentic behavior](#) on Facebook and Instagram. In October, we removed 14 networks of accounts, Pages and Groups. Eight of them — from Georgia, Myanmar, Ukraine, and Azerbaijan — targeted domestic audiences in their own countries, and six networks — from Iran, Egypt, US, and Mexico — focused on people outside of their country. This October report includes 7 networks we already announced on [October 8](#) and [October 27](#), and 6 new networks.

- **Total number of Facebook accounts removed:** 1,196
- **Total number of Instagram accounts removed:** 994
- **Total number of Pages removed:** 7,947
- **Total number of Groups removed:** 110

We are making progress rooting out this abuse, but as we've said before, it's an ongoing effort. We're committed to continually improving to stay ahead. That means building better technology, hiring more people and working closely with law enforcement, security experts and other companies.

#### Networks removed in October 2020:

1. **NEW Iran:** We removed 12 Facebook accounts, two Pages and 307 Instagram accounts linked to individuals associated with EITRC, a Tehran-based IT company. This activity originated in Iran and targeted primarily Israel, and also Iraq. This network was early in its audience building when we removed it. We found this activity as part of our investigation into suspected coordinated inauthentic behavior in the region.
2. **NEW Iran, Afghanistan:** We removed 33 Facebook accounts, 11 Pages, six Groups and 47 Instagram accounts operated by individuals in Iran and Afghanistan. They targeted Farsi/Dari-speaking audiences primarily in Afghanistan. We found this network as part of our internal investigation into suspected coordinated inauthentic behavior in the region.
3. **NEW Egypt, Turkey and Morocco:** We removed 31 Facebook accounts, 25 Pages and two Instagram accounts operated by individuals in Egypt, Turkey and Morocco associated with the Muslim Brotherhood. They targeted Egypt, Libya, Tunisia, Yemen, Somalia and Saudi Arabia. We found this network as part of our internal investigation into suspected coordinated inauthentic behavior in the region.
4. **NEW Georgia:** We removed 50 Facebook accounts, 49 Pages, four Groups, eight Events and 19 Instagram accounts linked to Alt-Info, a media entity in Georgia. This activity originated in the country of Georgia and targeted domestic audiences in Georgia. Alt-Info is now banned from Facebook. We found this network as part of our investigation into suspected coordinated inauthentic behavior in the region. Our assessment benefited from public reporting by the International Society for Fair Elections and Democracy (ISFED), a non-profit in Georgia.
5. **NEW Georgia:** We removed 54 Facebook accounts, 14 Pages, two Groups and 21 Instagram accounts linked to two political parties in Georgia — Alliance of Patriots and Georgian Choice. This activity originated in the country of Georgia and targeted domestic audiences in Georgia. We found this network after reviewing information about some of its activity publicly reported by the International Society for Fair Elections and Democracy (ISFED), a non-profit in Georgia.



6. **NEW Myanmar:** We removed 36 Facebook accounts, six Pages, two Groups and one Instagram account linked to Openmind, a PR agency in Myanmar. This activity originated in Myanmar and targeted domestic audiences in Myanmar. We found this network as part of our proactive investigation into suspected coordinated inauthentic behavior in the region ahead of the November election in Myanmar.
7. **NEW Ukraine:** We removed 46 Facebook accounts, 44 Pages, one Group and three Instagram accounts linked to MAS Agency, a PR firm in Ukraine, and individuals associated with Yulia Tymoshenko's campaign and Batkivshchyna, a political party in Ukraine. This activity originated in Ukraine and targeted domestic audiences in Ukraine. We found this network as part of our investigation into suspected coordinated inauthentic behavior in the region. Our review benefited from public reporting on some of this activity in Ukraine.
8. **Mexico, Venezuela:** We removed 2 Facebook Pages and 22 Instagram accounts operated by individuals from Mexico and Venezuela. They primarily targeted the US. We began this investigation based on information about this network's off-platform activity from the FBI. Our internal investigation revealed the full scope of this network on Facebook. **(Originally [announced on October 27, 2020](#))**
9. **Iran:** We also removed 12 Facebook accounts, 6 Pages and 11 Instagram accounts linked to individuals associated with the Iranian government. This small network originated in Iran and focused primarily on the US and Israel. It had some limited links to the CIB network we removed in [April 2020](#). We began this investigation based on information from the FBI about this network's off-platform [activity](#). **(Originally [announced on October 27, 2020](#))**
10. **Myanmar:** We removed 10 Facebook accounts, 8 Pages, 2 Groups and 2 Instagram accounts operated by individuals in Myanmar. They focused on domestic audiences. We found this network as part of our proactive investigation into suspected coordinated inauthentic behavior ahead of the upcoming election in the region. **(Originally [announced on October 27, 2020](#))**
11. **US:** We removed 202 Facebook accounts, 54 Pages and 76 Instagram accounts linked to Rally Forge, a US marketing firm, working on behalf of Turning Point USA and Inclusive Conservation Group. They focused primarily on domestic US audiences and also on Kenya and Botswana. Rally Forge is now banned from Facebook. We began our investigation after public reporting about some elements of this activity by the Washington Post. We are continuing to review all linked networks, and will take action as appropriate if we determine they are engaged in deceptive behavior. **(Originally [announced on October 8, 2020](#))**
12. **Myanmar:** We removed 38 Facebook accounts, 15 Pages and 6 Instagram accounts linked to members of the Myanmar military. This activity originated in Myanmar and targeted domestic audiences. We began our investigation after reviewing local public reporting about some elements of this activity as part of our proactive work ahead of the upcoming election in Myanmar. **(Originally [announced on October 8, 2020](#))**
13. **Azerbaijan:** We removed 589 Facebook accounts, 7,665 Pages and 437 accounts on Instagram linked to the Youth Union of New Azerbaijani Party. This network originated in Azerbaijan and focused primarily on domestic audiences. We identified this network through an internal investigation into suspected fake engagement activity in the region. **(Originally [announced on October 8, 2020](#))**
14. **Nigeria:** We removed 78 Facebook accounts, 45 Pages, 93 Groups and 46 Instagram accounts linked to the Islamic Movement in Nigeria. This network originated primarily in Nigeria and focused on domestic audiences. We identified this activity through our investigation into suspected coordinated inauthentic behavior in the region with some limited links to the [network we removed](#) in March 2019. **(Originally [announced on October 8, 2020](#))**

Here's a link to our full October CIB Report: <https://about.fb.com/news/2020/11/october-2020-cib-report/>

We shared information about these networks with researchers from Graphika, DFRLab, and Stanford's Internet Observatory and their reports on some of the new networks can be expected in the coming days.

Research announcements from announcements in the month of October can be found below:

- Stanford Internet Observatory's report on the US network (October 8): <https://cyber.fsi.stanford.edu/.../oct-2020-fb-rallev-forge>
- Graphika's report on the Myanmar network (October 8): <https://graphika.com/reports/myanmar-military-network/>
- DFRLab's report on the Russian domestic CIB network (October 8): <https://medium.com/dfrlab/facebook-removed-inauthentic-network-connected-to-united-russia-party-6b9cfd2332de>

- Graphika's report on the Mexico/Venezuela network (October 27): <https://graphika.com/reports/the-case-of-the-inauthentic-reposting-activists/>

Let me know if you have any questions.

Best,



---

**From:** Scully, Brian [/O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=7CA10604AEE04B1DAB53DC9F884130BD-SCULLY, BRI]  
**Sent:** 10/23/2020 10:01:16 AM  
**To:** [REDACTED]@twitter.com]  
**Subject:** RE: ISAC

Great. I'm trying to work on finding out if it's been sent separately, so at least I can give you a heads up. Hopefully we can get better at that as I'm trying not to drown you all.

Brian

---

**From:** [REDACTED]@twitter.com>  
**Sent:** Friday, October 23, 2020 9:59 AM  
**To:** Scully, Brian [REDACTED]@cisa.dhs.gov>  
**Subject:** Re: ISAC

**CAUTION:** This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

OK, we got that one already :)

Keep sending them our way. Impossible to know what we have and have not received.

On Fri, Oct 23, 2020 at 9:58 AM Scully, Brian [REDACTED]@cisa.dhs.gov> wrote:

Yep.

---

**From:** [REDACTED]@twitter.com>  
**Sent:** Friday, October 23, 2020 9:58 AM  
**To:** Scully, Brian [REDACTED]@cisa.dhs.gov>  
**Subject:** Re: ISAC

**CAUTION:** This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Wait, is it onen from Maryland Board of Elections?

On Fri, Oct 23, 2020 at 9:56 AM Scully, Brian [REDACTED]@cisa.dhs.gov> wrote:

Yes, CFITF is my team sending when I'm not doing it. Thanks, I'll add Misinformation Reports to our emails (will be sending one in a second).

Thanks [REDACTED]

Brian

**From:** [REDACTED]@twitter.com>  
**Sent:** Friday, October 23, 2020 9:55 AM  
**To:** Scully, Brian <[REDACTED]@cisa.dhs.gov>  
**Subject:** Re: ISAC

**CAUTION:** This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

No problem at all. I am getting a bunch of email from someone with CTIFC or something anyway? Is that you?

On Fri, Oct 23, 2020 at 9:53 AM Scully, Brian [REDACTED]@cisa.dhs.gov> wrote:

Hey Stacia,

Quick question for you – would you mind if I cc'd the ISAC on the reporting emails we send to Twitter? Right now, after I send an email to you, I send an email to the ISAC letting them know we reported. This would make things a bit more efficient on our end, but wanted to make sure you were comfortable with it before adding them.

Thanks,

Brian

Brian Scully

Chief, Countering Foreign Influence Task Force

DHS/CISA/NRMC

[REDACTED]@cisa.dhs.gov

Sent: 11/6/2020 12:20:13 PM  
To: [REDACTED]@fb.com]; [REDACTED]@fb.com]; [REDACTED]@fb.com]  
CC: CFITF [REDACTED]@hq.dhs.gov]  
Subject: RE: IG Disinfo Report

Hey Saléela,

In case it's helpful, just saw this debunking video on Twitter --  
<https://twitter.com/janeLytv/status/1324756117415776257?s=20>.

Brian

From: [REDACTED]@fb.com>  
Sent: Thursday, November 5, 2020 12:35 PM  
To: Scully, Brian [REDACTED]@cisa.dhs.gov>; [REDACTED]@fb.com>; [REDACTED]@fb.com>  
Cc: CFITF [REDACTED]@hq.dhs.gov>  
Subject: RE: IG Disinfo Report

**CAUTION:** This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Thank you, we will flag this for the teams!

From: Scully, Brian [REDACTED]@cisa.dhs.gov>  
Sent: Thursday, November 5, 2020 12:19 PM  
To: [REDACTED]@fb.com>; [REDACTED]@fb.com>; [REDACTED]@fb.com>  
Cc: CFITF [REDACTED]@hq.dhs.gov>  
Subject: IG Disinfo Report

Good afternoon Facebook,

Wanted to share this disinfo report about CISA and Director Krebs -- <https://www.instagram.com/p/CHNtFDPAUJH/>.

Regards,  
Brian

*The Cybersecurity and Infrastructure Security Agency (CISA) of the U.S. Department of Homeland Security (DHS) is not the originator of this information. CISA is forwarding this information, unedited, from its originating source - this information has not been originated or generated by CISA. This information may also be shared with law enforcement or intelligence agencies.*

*CISA affirms that it neither has nor seeks the ability to remove or edit what information is made available on social media platforms. CISA makes no recommendations about how the information it is sharing should be handled or used by social media companies. Additionally, CISA will not take any action, favorable or unfavorable, toward social media companies based on decisions about how or whether to use this information.*

*In the event that CISA follows up to request further information, such a request is not a requirement or demand. Responding to this request is voluntary and CISA will not take any action, favorable or unfavorable, based on decisions about whether or not to respond to this follow-up request for information.*

---

**From:** Scully, Brian [/O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=7CA10604AEE04B1DAB53DC9F884130BD-SCULLY, BRI]  
**Sent:** 11/10/2020 5:23:56 PM  
**To:** [REDACTED]@fb.com]  
**CC:** [REDACTED]@fb.com]  
**Subject:** RE: Hammer and scorecard narrative

I did.

---

**From:** [REDACTED]@fb.com>  
**Sent:** Tuesday, November 10, 2020 5:18 PM  
**To:** Scully, Brian [REDACTED]@cisa.dhs.gov>  
**Cc:** [REDACTED]@fb.com>  
**Subject:** Re: Hammer and scorecard narrative

**CAUTION:** This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Brian,

Also, just to confirm—will you let our USG partners know the meeting tomorrow is canx?

Thanks!

Sent from my iPhone

On Nov 10, 2020, at 4:10 PM, [REDACTED]@fb.com> wrote:

Many thanks for the quick reply.

Will let our partners know.

Enjoy your day!

Sent from my iPhone

On Nov 10, 2020, at 4:05 PM, Scully, Brian [REDACTED]@cisa.dhs.gov> wrote:

Yes, let's cancel please.

Brian Scully  
DHS Countering Foreign Interference Task Force  
National Risk Management Center  
[REDACTED]  
[REDACTED]@cisa.dhs.gov

---

**From:** [REDACTED]@fb.com>  
**Sent:** Tuesday, November 10, 2020 4:01:23 PM  
**To:** Scully, Brian [REDACTED]@cisa.dhs.gov>

Cc: [REDACTED]@fb.com>  
Subject: Re: Hammer and scorecard narrative

**CAUTION:** This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Brian—

One additional question. Given tomorrow is Veterans Day, will USG be available for our weekly call? Happy to canx so our federal partners can enjoy the holiday. Also wanted to ask so we could update our industry partners.

Thanks,  
[REDACTED]

Sent from my iPhone

On Nov 10, 2020, at 2:12 PM, Scully, Brian <[REDACTED]@cisa.dhs.gov> wrote:

This is very helpful Saleela. Thanks so much for sharing.

Brian

---

**From:** [REDACTED]@fb.com>  
**Sent:** Tuesday, November 10, 2020 2:11 PM  
**To:** Scully, Brian <[REDACTED]@cisa.dhs.gov>  
**Cc:** [REDACTED]@fb.com>; [REDACTED]@fb.com>  
**Subject:** RE: Hammer and scorecard narrative

**CAUTION:** This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Hi Brian,

Wanted to follow up on the below to say that our teams have confirmed that we have third-party fact-checker verification that the "Hammer and Scorecard" narrative is false and our systems are labeling and downranking the content as identified. FWIW, in comparison to other election-related misinformation hoaxes that we have been actively tracking, the level of virality is less. Our teams take this particular narrative, among others, very seriously, and are continuing to actively monitor and iterate on appropriately enforcing against this content.

Again, thank you for the collaboration and engagement here, we are grateful and appreciative.

Saleela

---

**From:** [REDACTED]@fb.com>  
**Sent:** Tuesday, November 10, 2020 10:12 AM  
**To:** Scully, Brian <[REDACTED]@cisa.dhs.gov> [REDACTED]@fb.com>; [REDACTED]@fb.com>  
**Subject:** Re: Hammer and scorecard narrative

Thank you, Brian. Our teams are actively monitoring developments on this at this time and to the extent you or USG have information about confirmed misinformation or other information of note, we absolutely welcome that for additional consideration and insight. Appreciate the ongoing collaboration very much.

---

**From:** Scully, Brian [REDACTED]@cisa.dhs.gov>  
**Sent:** Tuesday, November 10, 2020 9:24:57 AM  
**To:** [REDACTED]@fb.com>; [REDACTED]@fb.com>; [REDACTED]@fb.com>  
**Subject:** Hammer and scorecard narrative

Good morning,

Director Krebs is particularly concerned about the hammer and scorecard narrative that is making the rounds. Wanted to see if you all have been tracking this narrative and if there's anything you can share around amplification?

Thanks,  
Brian



---

**From:** Scully, Brian [REDACTED]@cisa.dhs.gov]  
**Sent:** 11/10/2020 6:44:54 PM  
**To:** [REDACTED]@twitter.com]  
**Subject:** Re: Hammer and scorecard narrative

Will do [REDACTED] Thank you!

Brian Scully  
DHS Countering Foreign Interference Task Force  
National Risk Management Center  
[REDACTED]  
[REDACTED]@cisa.dhs.gov

---

**From:** [REDACTED]@twitter.com>  
**Sent:** Tuesday, November 10, 2020 6:43:22 PM  
**To:** Scully, Brian [REDACTED]@cisa.dhs.gov>  
**Subject:** Re: Hammer and scorecard narrative

**CAUTION:** This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Hi Brian, hope you are well. Just a quick heads up, Politico published this [piece](#) about Director Krebs a few minutes ago. We noticed that one of his Tweets had been incorrectly labeled by our automated systems. We removed the label as soon as we noticed the issue. Please apologize to the Director on Twitter's behalf.

Thank you,  
[REDACTED]

On Tue, Nov 10, 2020 at 12:25 PM Scully, Brian <[REDACTED]@cisa.dhs.gov> wrote:

Yoel,

Thanks so much for the detailed response...very helpful. Will certainly pass anything we come across your way.

Brian

---

**From:** [REDACTED] [REDACTED]@twitter.com>  
**Sent:** Tuesday, November 10, 2020 12:20 PM  
**To:** Scully, Brian [REDACTED]@cisa.dhs.gov>  
**Cc:** [REDACTED]@twitter.com>; [REDACTED]@twitter.com>  
**Subject:** Re: Hammer and scorecard narrative

**CAUTION:** This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Hey Brian,

Sorry about the slow response - another crazy morning.

We've been tracking the Hammer/Scorecard issue closely, particularly since Director Krebs's tweet on the subject (which was pretty unambiguous as debunks go). We broadly labeled the conspiracy theory several days ago, pursuant to our policies. Once we enabled labeling, though, a 4chan-driven troll campaign kicked off, trying to reverse engineer our labeling logic and get labels to show up on unrelated tweets... which led to us turning off the automated labeling. We're going to backfill labels in bulk today for the period the automated labeling was disabled, but unfortunately we're in a bit of a cat-and-mouse situation where our ability to mitigate the conspiracy is tangled up in a clear attempt to work the ref by gaming our enforcements.

Let us know if there are especially high-profile examples of tweets sharing the conspiracy that *haven't* been labeled - we've been manually monitoring high-profile examples even once we disabled the automation, but it could be some slipped through the cracks.

Thanks,

██████████

On Tue, Nov 10, 2020 at 6:36 AM Scully, Brian ██████████@cisa.dhs.gov> wrote:

Thanks ██████████

---

**From:** ██████████@twitter.com>  
**Sent:** Tuesday, November 10, 2020 9:35 AM  
**To:** Scully, Brian ██████████@cisa.dhs.gov>  
**Cc:** ██████████@twitter.com>  
**Subject:** Re: Hammer and scorecard narrative

**CAUTION:** This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

We have been tracking this issue. I will allow ██████████ to follow up with detailed information.

Thanks,

██████████

On Tue, Nov 10, 2020 at 9:22 AM Scully, Brian ██████████@cisa.dhs.gov> wrote:

Good morning,

Director Krebs is very concerned about the hammer and scorecard narrative that's been making the rounds. Wondering if you all have been tracking that one and if there's anything you could share in terms of sharing and amplification?

Thanks,  
Brian

**From:** [REDACTED]@twitter.com]  
**Sent:** 11/13/2020 11:36:32 PM  
**To:** Scully, Brian [REDACTED]@cisa.dhs.gov]  
**Subject:** Re: FW: Twitter Assistance

**CAUTION:** This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

We have labeled so many Tweets tonight, so I am afraid that for now the answer is that it isn't ending tonight. Talk soon!

On Fri, Nov 13, 2020 at 11:35 PM Scully, Brian <[REDACTED]@cisa.dhs.gov> wrote:

Ugh...do you all ever stop testifying?!? Good luck. You hang in there as well...the election has to end at some point, right? Right?

**From:** [REDACTED]@twitter.com>  
**Sent:** Friday, November 13, 2020 11:33 PM  
**To:** Scully, Brian <[REDACTED]@cisa.dhs.gov>  
**Subject:** Re: FW: Twitter Assistance

**CAUTION:** This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Man, my boss testifies on Tuesday in front of Judiciary and I am so tired of working. Let's just hope tomorrow stays calm. Hang in there!

On Fri, Nov 13, 2020 at 11:26 PM Scully, Brian <[REDACTED]@cisa.dhs.gov> wrote:

Some Friday night fun for the two of us! 😊 Hope you are well.

Brian

**From:** [REDACTED]@twitter.com>  
**Sent:** Friday, November 13, 2020 11:21 PM  
**To:** Scully, Brian [REDACTED]@cisa.dhs.gov>  
**Cc:** [REDACTED]@twitter.com>; CFITF <[REDACTED]@hq.dhs.gov>  
**Subject:** Re: FW: Twitter Assistance

**CAUTION:** This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Thanks Brian, we will escalate.

On Fri, Nov 13, 2020 at 11:20 PM Scully, Brian <[REDACTED]@cisa.dhs.gov> wrote:

██████ and ██████

Please see below report from Dominion regarding disinformation about the location of servers. For awareness, I redacted a second tweet based on legal guidance.

Regards,

Brian

*The Cybersecurity and Infrastructure Security Agency (CISA) of the U.S. Department of Homeland Security (DHS) is not the originator of this information. CISA is forwarding this information from its originating source – this information has not been originated or generated by CISA. This information may also be shared with law enforcement or intelligence agencies.*

*CISA affirms that it neither has nor seeks the ability to remove or edit what information is made available on social media platforms. CISA makes no recommendations about how the information it is sharing should be handled or used by social media companies. Additionally, CISA will not take any action, favorable or unfavorable, toward social media companies based on decisions about how or whether to use this information.*

*In the event that CISA follows up to request further information, such a request is not a requirement or demand. Responding to this request is voluntary and CISA will not take any action, favorable or unfavorable, based on decisions about whether or not to respond to this follow-up request for information.*

**From:** Kay Stimson ██████@dominionvoting.com>  
**Sent:** Friday, November 13, 2020 10:57:02 PM  
**To:** Masterson, Matthew ██████@cisa.dhs.gov>  
**Subject:** Twitter Assistance

**CAUTION:** This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Matt,

Can you assist with flagging this election disinformation content? It's patently false. Dominion has no server in Germany, and you should be able to confirm with DOD that this is untrue. Looks like it's recycling old viral claims and/or newer false claims posted to a disinformation website called thedonald.win, which we have also reported. Since the thread claims this is an Amazon server and it looks like others are saying this, you should be able to check with them to confirm this is fake news as well. Thanks.

Tweet to Report:

[Redacted]

Tweet with Link to Recycled/Viral Rumor:

<https://twitter.com/cody41263233/status/1327421997782093830/photo/1>

Thanks,  
Kay

**KAY STIMSON** | VP, GOVERNMENT AFFAIRS

DOMINION VOTING SYSTEMS

[DOMINIONVOTING.COM](https://www.dominionvoting.com)

**From:** [REDACTED]@twitter.com]  
**Sent:** 11/14/2020 11:25:52 AM  
**To:** Scully, Brian [REDACTED]@cisa.dhs.gov]  
**CC:** CFITF [REDACTED]@hq.dhs.gov]; [REDACTED]@twitter.com]  
**Subject:** Re: FW: Twitter Assistance

**CAUTION:** This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Thank you, Brian. This Tweet has been labeled.

On Fri, Nov 13, 2020 at 11:20 PM [REDACTED]@twitter.com> wrote:  
Thanks Brian, we will escalate.

On Fri, Nov 13, 2020 at 11:20 PM Scully, [REDACTED]@cisa.dhs.gov> wrote:  
[REDACTED] and [REDACTED]

Please see below report from Dominion regarding disinformation about the location of servers. For awareness, I redacted a second tweet based on legal guidance.

Regards,  
Brian

*The Cybersecurity and Infrastructure Security Agency (CISA) of the U.S. Department of Homeland Security (DHS) is not the originator of this information. CISA is forwarding this information from its originating source – this information has not been originated or generated by CISA. This information may also be shared with law enforcement or intelligence agencies.*

*CISA affirms that it neither has nor seeks the ability to remove or edit what information is made available on social media platforms. CISA makes no recommendations about how the information it is sharing should be handled or used by social media companies. Additionally, CISA will not take any action, favorable or unfavorable, toward social media companies based on decisions about how or whether to use this information.*

*In the event that CISA follows up to request further information, such a request is not a requirement or demand. Responding to this request is voluntary and CISA will not take any action, favorable or unfavorable, based on decisions about whether or not to respond to this follow-up request for information.*

**From:** Kay Stimson <[REDACTED]@dominionvoting.com>  
**Sent:** Friday, November 13, 2020 10:57:02 PM  
**To:** Masterson, Matthew <[REDACTED]@cisa.dhs.gov>  
**Subject:** Twitter Assistance

**CAUTION:** This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Matt,

Can you assist with flagging this election disinformation content? It's patently false. Dominion has no server in Germany, and you should be able to confirm with DOD that this is untrue. Looks like it's recycling old viral claims and/or newer false claims posted to a disinformation website called thedonald.win, which we have also reported. Since the thread claims this is an Amazon server and it looks like others are saying this, you should be able to check with them to confirm this is fake news as well. Thanks.

Tweet to Report:

[Redacted]

Tweet with Link to Recycled/Viral Rumor:

<https://twitter.com/cody41263233/status/1327421997782093830/photo/1>

Thanks,  
Kay

**KAY STIMSON** | VP, GOVERNMENT AFFAIRS  
DOMINION VOTING SYSTEMS  
[REDACTED] | [DOMINIONVOTING.COM](https://www.dominionvoting.com)



---

**From:** Scully, Brian [REDACTED]@cisa.dhs.gov]  
**Sent:** 11/3/2020 3:42:16 PM  
**To:** [REDACTED]@fb.com]; Masterson, Matthew [REDACTED]@cisa.dhs.gov]  
**CC:** [REDACTED]@fb.com]  
**Subject:** Re: Election Misinformation Confirmation Requested

Let me check. I'm being told PA is going to put out a statement on it shortly.

Brian Scully  
DHS Countering Foreign Interference Task Force  
National Risk Management Center  
[REDACTED]  
[REDACTED]@cisa.dhs.gov

---

**From:** [REDACTED]@fb.com>  
**Sent:** Tuesday, November 3, 2020 3:39:57 PM  
**To:** Scully, Brian [REDACTED]@cisa.dhs.gov>; Masterson, Matthew [REDACTED]@cisa.dhs.gov>  
**Cc:** [REDACTED]@fb.com>  
**Subject:** Re: Election Misinformation Confirmation Requested

**CAUTION:** This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Both, actually, if you might know?

---

**From:** Scully, Brian [REDACTED]@cisa.dhs.gov>  
**Sent:** Tuesday, November 3, 2020 3:37:01 PM  
**To:** [REDACTED]@fb.com>; Masterson, Matthew [REDACTED]@cisa.dhs.gov>  
**Cc:** [REDACTED]@fb.com>  
**Subject:** Re: Election Misinformation Confirmation Requested

Hi [REDACTED]

The poll worker destroying ballots is disinfo. It are you asking about whether or not the person was a poll worker?

Brian

Brian Scully  
DHS Countering Foreign Interference Task Force  
National Risk Management Center  
[REDACTED]  
[REDACTED]@cisa.dhs.gov

---

**From:** [REDACTED]@fb.com>  
**Sent:** Tuesday, November 3, 2020 3:31:26 PM  
**To:** Scully, Brian [REDACTED]@cisa.dhs.gov>; Masterson, Matthew [REDACTED]@cisa.dhs.gov>  
**Cc:** [REDACTED]@fb.com>  
**Subject:** Election Misinformation Confirmation Requested

**CAUTION:** This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Hi Brian and Matt,

Can you please confirm the below is election misinformation?

<https://mobile.twitter.com/peterjhasson/status/1323716141202739201?s=21>

Thank You,  
[REDACTED]

---

**From:** Scully, Brian [/O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=7CA10604AEE04B1DAB53DC9F884130BD-SCULLY, BRI]  
**Sent:** 11/6/2020 12:22:04 PM  
**To:** [REDACTED]@twitter.com]; [REDACTED]@twitter.com]; [REDACTED]@twitter.com]; Twitter Government & Politics [gov@twitter.com]  
**CC:** CFITF [REDACTED]@hq.dhs.gov  
**Subject:** FW: Delaware County's response to video circulating of ballots

Twitter,

FYI – Delaware County, PA is debunking the below video.

Regards,  
Brian

---

**From:** Masterson, Matthew <[REDACTED]@cisa.dhs.gov>  
**Sent:** Friday, November 6, 2020 12:20 PM  
**To:** Scully, Brian <[REDACTED]@cisa.dhs.gov>; Dragseth, John <[REDACTED]@cisa.dhs.gov>  
**Subject:** FW: Delaware County's response to video circulating of ballots

Brian and John,

Please see below from Delaware County PA debunking those videos I provided earlier. Can you provide to platforms as additional context?

Matthew V. Masterson  
Senior Cybersecurity Advisor  
Department of Homeland Security  
Cybersecurity & Infrastructure Security Agency (CISA)

[REDACTED]  
[\[REDACTED\]@hq.dhs.gov](mailto:[REDACTED]@hq.dhs.gov)

---

**From:** Myers, Jessica <[REDACTED]@pa.gov>  
**Sent:** Friday, November 6, 2020 12:00 PM  
**To:** Masterson, Matthew <[REDACTED]@cisa.dhs.gov>  
**Subject:** Fwd: Delaware County's response to video circulating of ballots

**CAUTION:** This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

FYI  
Jessica C. Myers  
Director of Policy  
PA Department of State  
[REDACTED]

**From:** Yabut, Danilo [REDACTED]@pa.gov>  
**Sent:** Friday, November 6, 2020 11:59:33 AM  
**To:** Myers, Jessica [REDACTED]@pa.gov>  
**Subject:** FW: Delaware County's response to video circulating of ballots

**From:** Yabut, Danilo  
**Sent:** Friday, November 6, 2020 11:50 AM  
**To:** Degraffenreid, Veronica [REDACTED]@pa.gov>; Boockvar, Kathryn [REDACTED]@pa.gov>; Stevens, Sari [REDACTED]@pa.gov>; Marks, Jonathan [REDACTED]@pa.gov>; Murren, Wanda [REDACTED]@pa.gov>; Gates, Timothy [REDACTED]@pa.gov>; Kotula, Kathleen [REDACTED]@pa.gov>  
**Cc:** Lyon, Ellen <[REDACTED]@pa.gov>; Humphrey, Laura <[REDACTED]@pa.gov>; Parker, Scott [REDACTED]@pa.gov>; Paz, Darwin <[REDACTED]@pa.gov>  
**Subject:** RE: Delaware County's response to video circulating of ballots

FYI: regarding this, they posted this on facebook:  
<https://www.facebook.com/DelawareCountyCouncil/posts/1883402795141692>

Dan

**From:** Degraffenreid, Veronica <[REDACTED]@pa.gov>  
**Sent:** Friday, November 6, 2020 11:45 AM  
**To:** Boockvar, Kathryn <[REDACTED]@pa.gov>; Stevens, Sari <[REDACTED]@pa.gov>; Marks, Jonathan [REDACTED]@pa.gov>; Murren, Wanda [REDACTED]@pa.gov>; Yabut, Danilo [REDACTED]@pa.gov>; Gates, Timothy <[REDACTED]@pa.gov>; Kotula, Kathleen <[REDACTED]@pa.gov>  
**Subject:** FW: Delaware County's response to video circulating of ballots

**Veronica W. Degraffenreid | Special Advisor for Elections Modernization**  
 Pennsylvania Department of State

Office: [REDACTED] | Mobile: [REDACTED] | Email: [REDACTED]

**From:** Reuther, Christine <[REDACTED]@co.delaware.pa.us>  
**Sent:** Friday, November 6, 2020 11:44 AM  
**To:** Degraffenreid, Veronica <[REDACTED]@pa.gov>  
**Subject:** Fwd: Delaware County's response to video circulating of ballots

Fyi.

Get [Outlook for Android](#)

**From:** Marofsky, Adrienne <[REDACTED]@co.delaware.pa.us>  
**Sent:** Friday, November 6, 2020, 11:37 AM  
**To:** Zidek, Brian; Taylor, Monica; Madden, Kevin; Schaefer, Elaine; Reuther, Christine; Lazarus, Howard; Martin, William; [REDACTED]@duanemorris.com'; Stollsteimer, Jack; Rouse, Tanner; Jackson, Marianne A.; Hagan, Lauren T.  
**Cc:** Herlinger, Ryan; Morrone, Katherine; Cairry, Deborah  
**Subject:** Delaware County's response to video circulating of ballots

As you may know, video has been circulating of an election worker along with allegations of fraud. Below is the statement that we issued along with a screen shot from the actual live stream. Once we have the number of ballots damaged, I will edit the release. I needed to get this out asap to respond to dozens of press calls.

Manipulated video has been circulating online purporting to show Delaware County election staff fraudulently filling in blank ballots. The video was taken from the official live stream provided by Delaware County, however, the circulated video is zoomed in to crop out the surrounding area, including the bipartisan observers who were not more than six feet away and does not give the full picture of the process.

The cropped video portrays an election worker, seemingly alone at a table, marking a ballot. The actual video shows the election worker at a table with other coworkers in a room full of people with bipartisan observers a few feet away at each end of the table, closely observing the worker from approximately 6 feet away. This arrangement was agreed upon between the Election Bureau and the former Republican Chairman of Delaware County Council, acting in his capacity as counsel for the Delaware County Republican Party.

During the processing of ballots, a machine extractor opens the ballots. Some ballots were damaged by the extractor during this process in such a way that the ballots could not be scanned successfully. According to the scanner manufacturer, Hart, the best practice to deal with damaged ballots that cannot be scanned is to transcribe the votes on each ballot to a clean ballot and scan the clean ballot. In accordance with that guidance, the Chief Clerk of the Delaware County Bureau of Elections instructed elections staff to manually transcribe the damaged ballots. As ballots were being transcribed, the original damaged ballots were directly beside the new ballots and bipartisan observers witnessed the process at close range. Damaged ballots have been preserved.

The Delaware County Bureau of Elections has been offering a live-streaming of the counting of ballots, which began on Nov. 3. The video allows residents to watch the process in real-time and offers a transparent view of the process. Unfortunately, some residents have altered to video and are making false accusations, which baselessly and wrongly attacks the integrity of the election staff and the completely transparent process by which votes are being counted in Delaware County.

(The attached screen shot of the video shows the election worker at a table with other coworkers in a room full of people with bipartisan observers closely observing the worker.)

Sincerely,  
Adrienne Marofsky  
Public Relations Director for Delaware County

From: [REDACTED]@google.com]  
 Sent: 12/9/2020 9:09:29 AM  
 To: Scully, Brian [REDACTED]@cisa.dhs.gov]; Snell, Allison [REDACTED]@cisa.dhs.gov]; Schaul, Robert [REDACTED]@cisa.dhs.gov]  
 Subject: YouTube Policy Update

**CAUTION:** This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Good Morning,

I am writing to let you know about an update to YouTube's policies pertaining to election-related misinformation and to offer a briefing about these updates.

Beginning today, we will prohibit content alleging that widespread fraud or errors changed the outcome in any past US Presidential election. For example, we will remove videos claiming that a presidential candidate won the election as a result of widespread software glitches or counting errors. Given that states' certification of election results show that Biden has won, and our policies relating to misinformation about past elections now apply to content about the US 2020 presidential election uploaded beginning December 9. We will not issue any strikes to channels for removals between now and January 20. From January 20 forward, channels will be eligible to receive strikes for violative content they upload to YouTube. You can read more about our 2020 US election efforts in our blog post [here](#).

Best Regards,

Kevin

[REDACTED] Government Affairs & Public Policy Manager,  
 YouTube | [REDACTED]@google.com | [REDACTED]

**From:** [REDACTED]@twitter.com]  
**Sent:** 1/7/2021 10:58:39 PM  
**To:** Misinformation Reports [REDACTED]@cisecurity.org]  
**CC:** Scully, Brian [REDACTED]@cisa.dhs.gov]; [REDACTED]@twitter.com  
**Subject:** Re: FW: Election Related Misinformation

**CAUTION:** This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Thank you, Aaron. Both Tweets have been removed from the service.

Thank you,  
Stacia

On Thu, Jan 7, 2021 at 3:53 PM [REDACTED]@twitter.com> wrote:  
Thank you, Aaron. We will escalate.

Thanks,  
Stacia

On Thu, Jan 7, 2021 at 3:44 PM Misinformation Reports <[REDACTED]@cisecurity.org> wrote:  
Brian, Twitter,

Please see this report below from the Arizona SOS office. Please let me know if you have any questions.

Cc: [REDACTED], I am not sure the best contact email to send this to at Twitter.

Thanks,

Aaron

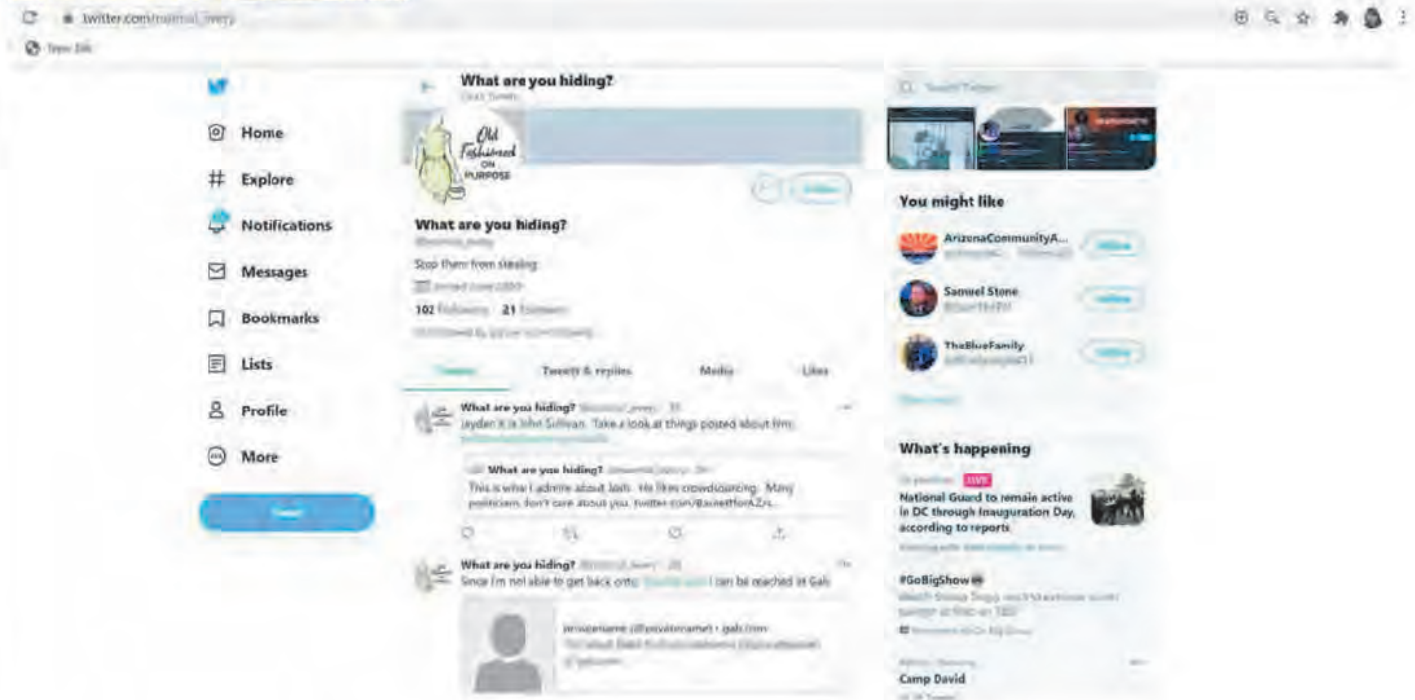
**From:** C.Murphy Hebert <[REDACTED]@azsos.gov>  
**Sent:** Thursday, January 7, 2021 3:26 PM  
**To:** Misinformation Reports <[REDACTED]@cisecurity.org>  
**Cc:** Ken Matta <[REDACTED]@azsos.gov>; Allie Bones <[REDACTED]@azsos.gov>  
**Subject:** Election Related Misinformation

Hello,

I'm Murphy Hebert, communications director for the Office of the Arizona Secretary of State.  
Email: [REDACTED]@azsos.gov

I am flagging this twitter account for your review. @normal\_every

[https://twitter.com/normal\\_every](https://twitter.com/normal_every)



Of specific concern to the Secretary of State are the following tweets:

[https://twitter.com/normal\\_every/status/1346451683384160257](https://twitter.com/normal_every/status/1346451683384160257)

[https://twitter.com/normal\\_every/status/1346233687160008704](https://twitter.com/normal_every/status/1346233687160008704)

Reason: These messages falsely assert that the Voter Registration System is owned and therefore operated by foreign actors.

This is an attempt to further undermine confidence in the election institution in Arizona.

Thank you for your consideration in reviewing this matter for action.

Sincerely,

C. Murphy Hebert  
Communications Director  
Arizona Secretary of State

.....

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

.....



**From:** [REDACTED]@fb.com]  
**Sent:** 5/4/2022 3:48:11 PM  
**To:** Protentis, Lauren [REDACTED]@cisa.dhs.gov]  
**CC:** Hale, Geoffrey (He/Him) [REDACTED]@cisa.dhs.gov]; Snell, Allison (She/Her) [REDACTED]@cisa.dhs.gov]; [REDACTED]@fb.com]; Schaul, Robert [REDACTED]@cisa.dhs.gov]; Scully, Brian [REDACTED]@cisa.dhs.gov]; Kuennen, David [REDACTED]@cisa.dhs.gov]; [REDACTED]@fb.com]; [REDACTED]@fb.com]  
**Subject:** Re: Account Security

Hello Team CISA!

Hope you are all well.

In our conversation a few weeks ago, you mentioned that your team could potentially help connect us with local election offices. Is this something you are still able to help with? Additionally, we can provide a training for them on account security best practices if you think that could be helpful.

And as always, if there is anything we can do to be helpful in the meantime, please let us know!

Thanks,

[REDACTED]

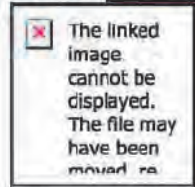
---

**From:** Protentis, Lauren [REDACTED]@cisa.dhs.gov>  
**Date:** Wednesday, April 27, 2022 at 12:37 PM  
**To:** [REDACTED]@fb.com>, [REDACTED]@fb.com>  
**Cc:** Hale, Geoffrey (He/Him) <[REDACTED]@cisa.dhs.gov>, Snell, Allison (She/Her) [REDACTED]@cisa.dhs.gov>, [REDACTED]@fb.com>, [REDACTED]@fb.com>, [REDACTED]@fb.com>, Schaul, Robert [REDACTED]@cisa.dhs.gov>, Scully, Brian [REDACTED]@cisa.dhs.gov>, Kuennen, David [REDACTED]@cisa.dhs.gov>  
**Subject:** Re: Account Security

Perfect thank you so much!

**Lauren Protentis • Mis, Dis, Malinformation Team • National Risk Management Center • Cybersecurity and Infrastructure Security Agency (CISA)**

M: [REDACTED] | E: [REDACTED]@cisa.dhs.gov | HSDN: [REDACTED]@dhs.gov | CLAN: [REDACTED]@dhs.ic.gov




---

**From:** [REDACTED]@fb.com>  
**Sent:** Wednesday, April 27, 2022 11:15:25 AM  
**To:** Protentis, Lauren [REDACTED]@cisa.dhs.gov>; [REDACTED]@fb.com>

Cc: Hale, Geoffrey (He/Him) <[redacted]@cisa.dhs.gov>; Snell, Allison (She/Her) <[redacted]@cisa.dhs.gov>; [redacted]@fb.com>; [redacted]@fb.com>; [redacted]@fb.com>; [redacted]@fb.com>; [redacted]@fb.com>; Schaul, Robert <[redacted]@cisa.dhs.gov>; Scully, Brian <[redacted]@cisa.dhs.gov>; Kuennen, David <[redacted]@cisa.dhs.gov>

Subject: Re: Account Security

Got it – and no problem! I had our team design my email directly into the document (new version attached here) so everything is all in one place for you.

Best,



[redacted]  
State and Local Politics & Government Outreach  
[redacted]@fb.com

---

From: Protentis, Lauren <[redacted]@cisa.dhs.gov>  
Date: Wednesday, April 20, 2022 at 12:45 PM  
To: [redacted]@fb.com>, [redacted]@fb.com>  
Cc: Hale, Geoffrey (He/Him) <[redacted]@cisa.dhs.gov>, Snell, Allison (She/Her) <[redacted]@cisa.dhs.gov>, [redacted]@fb.com>, [redacted]@fb.com>, [redacted]@fb.com>, [redacted]@fb.com>, Schaul, Robert <[redacted]@cisa.dhs.gov>, Scully, Brian <[redacted]@cisa.dhs.gov>, Kuennen, David <[redacted]@cisa.dhs.gov>  
Subject: RE: Account Security

Hi [redacted] That could work, though we'd also welcome that as part of the document. Given we have a broader team that does trainings etc, it might be helpful for that info to be included in the doc. Though I understand there may be concerns with this approach.

Will take your steer, let me know what you think.

Lauren Protentis (She/Her)  
Mis, Dis, and Mal-information (MDM) Team  
Election Security Initiative  
National Risk Management Center  
Cybersecurity and Infrastructure Security Agency  
O: [redacted] | Email: [redacted]@cisa.dhs.gov | HSDN: [redacted]@dhs.gov | CLAN: [redacted]@dhs.ic.gov



---

From: [redacted]@fb.com>  
Sent: Monday, April 18, 2022 5:30 PM  
To: [redacted]@fb.com>; Protentis, Lauren <[redacted]@cisa.dhs.gov>  
Cc: Hale, Geoffrey (He/Him) <[redacted]@cisa.dhs.gov>; Snell, Allison (She/Her) <[redacted]@cisa.dhs.gov>; [redacted]@fb.com>; [redacted]@fb.com>; [redacted]@fb.com>; [redacted]@fb.com>; Schaul, Robert <[redacted]@cisa.dhs.gov>; Scully, Brian <[redacted]@cisa.dhs.gov>

<[REDACTED]@cisa.dhs.gov>; Kuennen, David <[REDACTED]@cisa.dhs.gov>

**Subject:** Re: Account Security

Thanks Lauren!

Would it work to just provide my email when you share out this one pager, and let them know if they need anything (like a page verification) or have any content they want to escalate for review, they can reach out to me and I can get them to the right person to help?

Best,

 Meta

Eya Guidarini

State and Local Politics & Government Outreach

---

**From:** [REDACTED]@fb.com>

**Date:** Monday, April 18, 2022 at 11:50 AM

**To:** Protentis, Lauren <[REDACTED]@cisa.dhs.gov>

**Cc:** Hale, Geoffrey (He/Him) <[REDACTED]@cisa.dhs.gov>, Snell, Allison (She/Her)

<[REDACTED]@cisa.dhs.gov>, [REDACTED]@fb.com>, [REDACTED]

<[REDACTED]@fb.com>, [REDACTED]@fb.com>, [REDACTED]@fb.com>, [REDACTED]

<[REDACTED]@fb.com>, Schaul, Robert <[REDACTED]@cisa.dhs.gov>, Scully, Brian <[REDACTED]@cisa.dhs.gov>,

Kuennen, David <[REDACTED]@cisa.dhs.gov>

**Subject:** Re: Account Security

Great! Many thank, Lauren for the quick reply & feedback.

[REDACTED] – who is cc'd on our team will loop in others from her team

Happy to move some of your colleagues to BCC as needed/defer to you to do that as [REDACTED] and her team work out the details.

Sent from my iPhone

On Apr 18, 2022, at 10:54 AM, Protentis, Lauren <[REDACTED]@cisa.dhs.gov> wrote:

Thanks so much for sending, [REDACTED]!

This looks great – the only thing I'd recommend adding is any steps for flagging or escalating MDM content, if possible. I think then that would make this a comprehensive product on both of the critical needs for officials – account security and MDM concerns. We discussed this a bit in our in-person meeting two weeks ago. Let me know if that's doable.

Thank you!

Lauren Protentis (She/Her)

Mis, Dis, and Mal-information (MDM) Team

Election Security Initiative

National Risk Management Center  
Cybersecurity and Infrastructure Security Agency

O: [REDACTED] | Email: [REDACTED]@cisa.dhs.gov | HSDN: [REDACTED]@dhs.sgov.gov | CLAN:  
[REDACTED]@dhs.ic.gov

**From:** [REDACTED]@fb.com>

**Sent:** Friday, April 15, 2022 9:01 AM

**To:** Protentis, Lauren <[REDACTED]@cisa.dhs.gov>; Hale, Geoffrey (He/Him) [REDACTED]@cisa.dhs.gov>; Snell, Allison (She/Her) <Allison.Snell@cisa.dhs.gov>

**Cc:** [REDACTED]@fb.com>; [REDACTED]@fb.com>; [REDACTED]@fb.com>; [REDACTED]@fb.com>; [REDACTED]@fb.com>

**Subject:** Account Security

**CAUTION:** This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Good Morning!

As discussed during our meeting last week, I wanted to share our account security doc that we've been working on.

We would be grateful for any feedback and would be happy to set up a call to discuss. I am including [REDACTED] & [REDACTED] who you met during our meeting & are helping implement these procedures with key stakeholders. Also, [REDACTED] to help schedule a call to discuss, if helpful.

Many thanks for your collaboration & best for a great weekend!

[REDACTED]

**From:** Protentis, Lauren [/O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=604C2D8C37944283805D4BD9A9A83476-LAUREN.PROT]  
**Sent:** 5/20/2022 10:35:56 AM  
**To:** [REDACTED]@microsoft.com]; [REDACTED] (CELA) [REDACTED]@microsoft.com]; Jeremy [REDACTED]@microsoft.com]; [REDACTED] (CELA) [REDACTED]@microsoft.com]  
**Subject:** RE: One-Pager for Elections Officials

Many, many thanks! Really appreciate it ☺

Lauren Protentis (She/Her)  
Mis, Dis, and Mal-information (MDM) Team  
Election Security Initiative  
National Risk Management Center  
Cybersecurity and Infrastructure Security Agency

O: [REDACTED] | Email: [REDACTED]@cisa.dhs.gov | HSDN: [REDACTED]@dhs.sgov.gov | CLAN: [REDACTED]@dhs.ic.gov



**From:** [REDACTED]@microsoft.com>  
**Sent:** Friday, May 20, 2022 9:59 AM  
**To:** Protentis, Lauren [REDACTED]@cisa.dhs.gov>; [REDACTED] (CELA) [REDACTED]@microsoft.com>; [REDACTED]@microsoft.com>; [REDACTED] (CELA) [REDACTED]@microsoft.com>  
**Subject:** RE: One-Pager for Elections Officials

**CAUTION:** This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Lauren,

Thanks for reaching out. Attached is Microsoft's 1 pager for inclusion. Please let us know if you have any questions.

[REDACTED]

[REDACTED]

Director of Information Integrity  
Democracy Forward Team (CELA)  
[REDACTED]@microsoft.com

**From:** Protentis, Lauren <[REDACTED]@cisa.dhs.gov>  
**Sent:** Thursday, May 19, 2022 11:14 AM  
**To:** [REDACTED] (CELA) <[REDACTED]@microsoft.com>; [REDACTED]@microsoft.com>; [REDACTED]@microsoft.com>  
**Subject:** [EXTERNAL] One-Pager for Elections Officials

Hi [REDACTED]

I hope this email finds you well! Not sure this ask is as relevant to Microsoft, but thought I'd check. Meta is working with industry partners to create one-pagers for elections officials (in the lead up to the midterms) that provide steps to create secure accounts and to report MDM. We'll be sharing these products at our various engagements with officials.

Given your operating model is different than social media platforms, I'm not sure this is relevant. But, if so, we'd be happy to receive one from Microsoft.

I've attached a few examples of what the other companies have done.

Thanks so much!

Lauren Protentis (She/Her)  
Mis, Dis, and Mal-information (MDM) Team  
Election Security Initiative  
National Risk Management Center  
Cybersecurity and Infrastructure Security Agency

O: [REDACTED] | Email: [REDACTED]@cisa.dhs.gov | HSDN: [REDACTED]@dhs.sgov.gov | CLAN:  
[REDACTED]@dhs.ic.gov



From: [redacted]@twitter.com]  
Sent: 5/12/2022 4:43:21 PM  
To: Protentis, Lauren [redacted]@cisa.dhs.gov]  
Subject: Re: Twitter POC  
Attachments: Election Officials Best Practices.pdf

Sure thing, here's the updated version!

On Thu, May 12, 2022 at 4:32 PM Protentis, Lauren <[redacted]@cisa.dhs.gov> wrote:  
That would be so helpful if you could add it to the doc, thank you!

**Lauren Protentis • Mis, Dis, Malinformation Team • National Risk Management Center • Cybersecurity and Infrastructure Security Agency (CISA)**

M: [redacted] | E: [redacted]@cisa.dhs.gov | HSDN: [redacted]@dhs.sgov.gov |  
CLAN: [redacted]@dhs.ic.gov



---

From: [redacted]@twitter.com>  
Sent: Thursday, May 12, 2022 1:48:06 PM  
To: Protentis, Lauren <[redacted]@cisa.dhs.gov>  
Subject: Re: Twitter POC

The best way for them to do that is to contact [redacted]@twitter.com, I can add that to the doc if that would be helpful

On Thu, May 12, 2022 at 2:16 PM Protentis, Lauren <[redacted]@cisa.dhs.gov> wrote:  
Actually one question: is there a way to include something about how to report disinformation?

**Lauren Protentis • Mis, Dis, Malinformation Team • National Risk Management Center • Cybersecurity and Infrastructure Security Agency (CISA)**

M: [redacted] | E: [redacted]@cisa.dhs.gov | HSDN: [redacted]@dhs.sgov.gov |  
CLAN: [redacted]@dhs.ic.gov



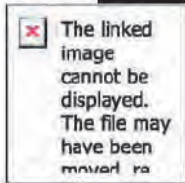
---

From: Protentis, Lauren <[redacted]@cisa.dhs.gov>  
Sent: Thursday, May 12, 2022 1:11:25 PM  
To: [redacted]@twitter.com>  
Subject: Re: Twitter POC

Thanks so much! Really appreciate it! State and local officials in NH and IL will be the first recipients of this, so thanks in advance.

**Lauren Protentis • Mis, Dis, Malinformation Team • National Risk Management Center • Cybersecurity and Infrastructure Security Agency (CISA)**

M: [REDACTED] | E: [REDACTED]@cisa.dhs.gov | HSDN: [REDACTED]@dhs.sgov.gov |  
CLAN: [REDACTED]@dhs.ic.gov



---

**From:** [REDACTED]@twitter.com>  
**Sent:** Thursday, May 12, 2022 7:40:47 AM  
**To:** Protentis, Lauren <[REDACTED]@cisa.dhs.gov>  
**Subject:** Re: Twitter POC

Hey Lauren,

Apologies for the delay, got final approval late last night. Here's a one-pager covering best practices, escalations, verification, and safety tools.

Thanks and let me know if you need anything else!

[REDACTED]

On Wed, May 11, 2022 at 10:39 AM [REDACTED]@twitter.com> wrote:  
Hey Lauren,

I'll have the one pager for you later today, just getting the final sign off before sending over

Thanks!

[REDACTED]

On Wed, May 11, 2022 at 9:09 AM Protentis, Lauren <[REDACTED]@cisa.dhs.gov> wrote:

Hi [REDACTED] and [REDACTED], Hope this email finds you well! Wanted to circle-back on this and see if you have any questions! The team has a few upcoming engagements with elections officials where this one-pager would be particularly helpful to share as a leave-behind.

All my best,

Lauren Protentis (She/Her)  
Mis, Dis, and Mal-information (MDM) Team  
Election Security Initiative  
National Risk Management Center



Cybersecurity and Infrastructure Security Agency

O: [REDACTED] | Email: [REDACTED]@cisa.dhs.gov | HSDN: [REDACTED]@dhs.sgov.gov |  
CLAN: [REDACTED]@dhs.ic.gov



**From:** Protentis, Lauren [REDACTED]@cisa.dhs.gov>  
**Sent:** Thursday, May 5, 2022 7:27 AM  
**To:** [REDACTED]@twitter.com>  
**Cc:** [REDACTED]@twitter.com>  
**Subject:** Re: Twitter POC

Great, thanks [REDACTED] and [REDACTED]

[REDACTED]: As referenced below, we're collecting one-pagers from our industry partners that illuminates best practices/instructions for account security, account verification, and reporting MDM, for elections officials. This will be a tool/resource we can share as we conduct trainings in advance of the midterms.

Let me know if you have any questions!

Laure

**Lauren Protentis • Mis, Dis, Malinformation Team • National Risk Management Center •  
Cybersecurity and Infrastructure Security Agency (CISA)**

M: [REDACTED] | E: [REDACTED]@cisa.dhs.gov | HSDN: [REDACTED]@dhs.sgov.gov |  
CLAN: [REDACTED]@dhs.ic.gov



---

**From:** [REDACTED]@twitter.com>  
**Sent:** Wednesday, May 4, 2022 4:53:00 PM  
**To:** Protentis, Lauren [REDACTED]@cisa.dhs.gov>  
**Cc:** [REDACTED]@twitter.com>  
**Subject:** Re: Twitter POC

Hi Lauren -

Glad to meet you; [REDACTED] from our team knows DHS very well from his time on the Hill. He's a great person to assist you on this.

Best,

TO

On Tue, May 3, 2022 at 1:20 PM Protentis, Lauren <[REDACTED]@cisa.dhs.gov> wrote:

Awesome! I'm meeting with Region 1 to include New Hampshire who mentioned that it was helpful for us to provide the verification information from Twitter last week. So, thanks again.

**Lauren Protentis • Mis, Dis, Malinformation Team • National Risk Management Center • Cybersecurity and Infrastructure Security Agency (CISA)**

M: [REDACTED] E: [REDACTED]@cisa.dhs.gov | HSDN: [REDACTED]@dhs.sgov.gov |

CLAN: [REDACTED]@dhs.ic.gov

---

**From:** [REDACTED]@twitter.com>

**Sent:** Tuesday, May 3, 2022 1:14:56 PM

**To:** Protentis, Lauren <[REDACTED]@cisa.dhs.gov>; [REDACTED]@twitter.com>

**Cc:** [REDACTED]@twitter.com>; [REDACTED]@twitter.com>

**Subject:** Re: Twitter POC

Hey Lauren,

Thanks for checking in on this. Adding [REDACTED] on our Public Policy team, who should be able to share our resources on this.

[REDACTED]

On Tue, May 3, 2022 at 10:14 AM Protentis, Lauren [REDACTED]@cisa.dhs.gov> wrote:

Hi [REDACTED] As mentioned in recent Industry Syncs, we're looking for one-pagers for elections officials that highlight platform best practices for getting verified (which you've provided below), account security and MDM reporting.

Is this something your team is able to pull together? I'm happy to share what others provided I'd that would be helpful to get you started.

Let me know if you have any questions!

**Lauren Protentis • Mis, Dis, Malinformation Team • National Risk Management Center • Cybersecurity and Infrastructure Security Agency (CISA)**

M: [REDACTED] E: [REDACTED]@cisa.dhs.gov | HSDN: [REDACTED]@dhs.sgov.gov |

CLAN: [REDACTED]@dhs.ic.gov

**From:** [REDACTED]@twitter.com>  
**Sent:** Wednesday, April 20, 2022 1:59:00 PM  
**To:** Protentis, Lauren <[REDACTED]@cisa.dhs.gov>  
**Cc:** [REDACTED]@twitter.com>; [REDACTED]@twitter.com>  
**Subject:** Re: FW: Twitter POC

**CAUTION:** This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Hey Lauren,

Government officials can apply through the public channel, or reach out by email to [gov@twitter.com](mailto:gov@twitter.com). Thanks!

[REDACTED]

On Wed, Apr 20, 2022 at 9:42 AM Protentis, Lauren <[REDACTED]@cisa.dhs.gov> wrote:

Greetings [REDACTED] and [REDACTED].

I suspect we'll receive this question more often as the midterms continue. A state elections agency in New Hampshire is inquiring about getting verified on Twitter.

In order for elections officials and state and local officials to verify their Twitter accounts, should we simply direct them to this information: [Twitter verification requirements - how to get the blue check](#)

Or is there another process or person you'd prefer we direct them towards?

Thank you!

Lauren Protentis (She/Her)

Mis, Dis, and Mal-information (MDM) Team

Election Security Initiative

National Risk Management Center

Cybersecurity and Infrastructure Security Agency

O: [REDACTED] | Email: [REDACTED]@cisa.dhs.gov | HSDN: [REDACTED]@dhs.sgov.gov |

CLAN: [REDACTED]@dhs.ic.gov



---

**From:** Moser, Michael (He/Him) <[REDACTED]@cisa.dhs.gov> **On Behalf Of** ElectionTaskForce  
**Sent:** Wednesday, April 20, 2022 11:00 AM  
**To:** Modricker, Daniel <[REDACTED]@cisa.dhs.gov>; Protentis, Lauren <[REDACTED]@cisa.dhs.gov>  
**Cc:** Tipton, James <[REDACTED]@cisa.dhs.gov>; ElectionTaskForce <[REDACTED]@cisa.dhs.gov>  
**Subject:** RE: Twitter POC

Hi Dan,

I'm adding Lauren Protentis to this chain, who's from our MDM team, to see if she may have some thoughts on how to proceed.

Kind Regards,

Mike Moser  
(He/Him)  
IT Cybersecurity Specialist (INFOSEC)  
Engagement, Assistance, and Training  
Election Security Initiative  
National Risk Management Center  
Cybersecurity and Infrastructure Security Agency  
M: [REDACTED] | [REDACTED]@cisa.dhs.gov



---

**From:** Modricker, Daniel <[REDACTED]@cisa.dhs.gov>  
**Sent:** Tuesday, April 19, 2022 8:22 PM  
**To:** ElectionTaskForce <[REDACTED]@cisa.dhs.gov>  
**Cc:** Tipton, James <[REDACTED]@cisa.dhs.gov>  
**Subject:** Twitter POC

Greetings,

During a meeting with a state elections partner we identified that their agency does not have the “verified identity” blue check for their Twitter account.

Is there a POC at Twitter to contact, or an expedited process for state elections agencies to pursue verification?

Best,  
Dan

**Daniel Modricker**

Outreach Coordinator, Region I

Cybersecurity and Infrastructure Security Agency

Cell: [REDACTED] | Email: [REDACTED]@hq.dhs.gov



**CISA**  
CYBER+INFRASTRUCTURE