No. 21-1387

In the Supreme Court of the United States

ERIK LECKNER,

Petitioner,

v.

GENERAL DYNAMICS, INC., GENERAL DYNAMICS INFORMATION TECHNOLOGY, INC., CSRA, LLC, ASGN, INC., APEX SYSTEMS, LLC,

Respondents.

On Petition for a Writ of Certiorari to the United States Court of Appeals for the Ninth Circuit

PETITION FOR REHEARING

ERIK LECKNER
PETITIONER PRO SE
747 S. MISSION ROAD
UNIT 2923
FALLBROOK, CA 92088
(760) 459-7772

JULY 22, 2022

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES ii

PREAMBLE 1

REASONS FOR REHEARING 3

CONCLUSION 15

RULE 44 CERTIFICATE 16

TABLE OF AUTHORITIES

Page

CASES

CBOCS West, Inc. v. Humphries,
553 U.S. 442, 128 S.Ct. 1951 (2008) 2

Clem and Spencer v. Computer Sciences Corp. (now known as GDIT), ARB No. 2020-0025, ALJ Nos. 2015-ERA-00003,-00004 1

Department of Homeland Security v. MacLean,
135 S.Ct. 913, 190 L.Ed.2d 771 (2015)..... 13

English v. General Elec. Co.,
496 U.S. 72 (1990) 2

Facebook Inc. v. Duguid,
926 F.3d 1146 (9th Cir. April 1, 2021)..... 13, 14

Gomez-Perez v. Potter,
553 U.S. 474 (2008) 3

Jackson v. Birmingham Board of Education,
544 U.S. 167 (2005) (Title IX) 2

Johnson v. Ry. Express Agency, Inc.,
421 U.S. 454, 95 S.Ct. 1716,
44 L.Ed.2d 295 (1975) 12, 13

Klopfenstein v. PCC Flow Technologies Holdings, Inc., ARB Case No. 04-149, 2004-SOX-11 (May 31, 2006) 8

Munsey v. Federal Mine Safety and Health Review Comm'n, 595 F.2d 735
(D.C. Cir. 1978)..... 14

NLRB v. Scrivener,
405 U.S. 117 (1972) 2

TABLE OF AUTHORITIES – Continued

Page

Passaic Valley Sewerage Comm. v. Dep't of Labor, 992 F.2d 474 (3rd Cir. 1993) 14

Smith v. Corning, 496 F.Supp. 2d 244 (W.D. NY 2007) 8

Sylvester v. Parexel International LLC, ARB No. 07-123, ALJ Nos. 2007-SOX-039 (ARB May 25, 2011) 14

United States ex rel. Brian Markus v. Aerojet Rocketdyne Holdings Inc., et al., Case No. 2:15-cv-02245-WBS-AC (E.D.Cal.) 9, 10

STATUTES

18 U.S.C. § 1514A(a) 1

18 U.S.C. § 1514A(a)(1) 9

18 U.S.C. § 1519 11

42 U.S.C. § 1981 3

JUDICIAL RULES

Sup. Ct. R. 44.1 3

Sup. Ct. R. 44.2 3

REGULATIONS

29 C.F.R. § 1980.103 11

29 C.F.R. § 1980.105(b) 12

TABLE OF AUTHORITIES – Continued

Page

CONGRESSIONAL DOCUMENTS

S.Rep. 107-146 (2002) 2

OTHER AUTHORITIES

CSRA Inc.,
U.S. Courts Award CSRA $57M Task Order to Secure IT Assets, (May 1, 2017), https://www.prnewswire.com/news-releases/us-courts-award-csra-57m-task-order-to-secure-it-assets-300448691.html..... 1

Office of Inspector General USEPA,
EPA Overpaid Invoices Due to Insufficient Contract Management Controls, May 20, 2019, https://www.epa.gov/sites/default/files/2019-05/documents/_epaoig_20190520-19-p-0157.pdf..... 8

Office of Public Affairs USDOJ,
Aerojet Rocketdyne Agrees to Pay $9 Million to Resolve False Claims Act Allegations of Cybersecurity Violations in Federal Government Contracts, July 8, 2022, https://www.justice.gov/opa/pr/aerojet-rocketdyne-agrees-pay-9-million-resolve-false-claims-act-allegations-cybersecurity 9

U.S. Dept. of Justice,
Deputy Attorney General Lisa O. Monaco Announces New Civil Cyber-Fraud Initiative, https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-

TABLE OF AUTHORITIES – Continued

Page

announces-new-civil-cyber-fraud-initiative 6

United States Supreme Court, https://www.supremecourt.gov/publicinfo/press/pressreleases/pr_05-03-22 (May 3, 2022) 4

PREAMBLE

The Supreme Court was recently breached. GDIT was previously responsible for securing IT assets of the U.S. Courts.[1] Security support is no better at the Supreme Court than it is at the U.S. EPA.

Whistleblowers who work in the cybersecurity and software industry who report wrongdoing are frequently subject to reprisals.[2] Recently, GDIT settled with the United States which alleged that GDIT submitted false claims and statements to DOE representing that the electronic medical records system was functional and would operate as intended and in accordance with contractual and DOE requirements.

It cannot be over-stated how vital are the avenues of legal redress to cybersecurity and software professionals, including rights available under each of the acts. Even under the best of circumstances, whistleblowers run enormous risks and suffer retaliation for reporting wrongdoing.

> Congress created the SOX whistleblower protection, 18 U.S.C. § 1514A(a), to address a culture, supported by law, that discourage[s] employees from reporting fraudulent behavior not only to the proper authorities . . . but even internally. This 'corporate code of silence' not only hampers investigations, but also creates

---

[1] *See* https://www.prnewswire.com/news-releases/us-courts-award-csra-57m-task-order-to-secure-it-assets-300448691.html.

[2] *See Clem and Spencer v. Computer Sciences Corp.* (now known as GDIT), ARB No. 2020-0025, ALJ Nos. 2015-ERA-00003,-00004.

> a climate where ongoing wrongdoing can occur with virtual impunity.

S.Rep. 107-146 (2002), at 5. Congress considered the whistleblower protection to be a "crucial" component of SOX for "restoring trust . . . by ensuring that corporate fraud and greed may be better detected, prevented, and prosecuted."

Regardless of the specific whistleblower law at issue in this matter, the principles setting forth the appropriate interpretation of protected activity are aligned, whether those activities occurred in the context of safety protection, complex cybersecurity and information technology, complex environmental protection or within the complex and highly regulated nuclear power industry.

To reach its tortured construction of SOX and the other relevant acts, the panel had to reject the historic broad construction of whistleblower protections by affirming the ALJ's statement that "SOX whistleblower protection does not extend to cybersecurity risks."

Previously, the Supreme Court and other federal courts have had no difficulty holding that whistle-blower provisions must be given broad scope to accomplish their remedial purposes. *NLRB v. Scrivener* (1972), 405 U.S. 117, 121-26; *English v. General Elec. Co.*, 496 U.S. 72, 82 (1990)(to "encourage" employees to report safety violations and protect their reporting activity).

Indeed, the public interest in protecting employees from reprisals is so strong that this Supreme Court has imputed a protection into laws that have no words creating it. *Jackson v. Birmingham Board of Education*, 544 U.S. 167 (2005) (Title IX); *CBOCS West, Inc. v. Humphries*, 553 U.S. 442, 128 S.Ct. 1951 (2008) (42

U.S.C. § 1981); *Gomez-Perez v. Potter*, 553 U.S. 474 (2008) (ADEA).

As the Supreme Court recognized, these protections for whistleblowers are necessary both for direct corporate employees, and employees who provide those services through contractor-vendors. If left standing, the decision will have a chilling effect detrimental to these laws' objective of increasing accountability, especially in the cybersecurity and software industry.

Pursuant to Rule 44.1, Petitioner respectfully petitions for a rehearing of the denial of a writ of certiorari to review the judgment of the Court of Appeals.

REASONS FOR REHEARING

Pursuant to Rule 44.2, there are numerous "intervening circumstances of a substantial or controlling effect" that arose subsequent to the completion of briefing at the certiorari stage and other substantial grounds not previously presented – that militate in favor of granting rehearing and certiorari, vacating the decision, and remanding for trial.

I

The Supreme Court was breached after completion of Leckner's petition at the certiorari stage. This was preventable by using a secure document repository. On May 3, 2022, Chief Justice Roberts issued the following public statement:

This was a singular and egregious [**security**] breach of that trust that is an affront to the Court and

the community of public servants who work here. https://www.supremecourt.gov/publicinfo/press/pressreleases/pr_05-03-22 (May 3, 2022).

In 2018, Leckner whistleblew that mission-critical federal information management systems lacked necessary cybersecurity controls for preventing sensitive data and information from being accessed, destroyed, leaked, printed, forwarded, and copied by unauthorized users. These controls were not in place due to GDIT's gross negligence. GDIT's cybersecurity infrastructure was so weak that there are no words for even describing it.

Leckner reported fraud and numerous cybersecurity breaches and risks, which included the Log4j cyber vulnerabilities, which recently caused massive cyber-attacks across the globe. The Log4j cyberattacks allowed for classified Ukraine defense ministry information to be accessed by foreign governments, using the same cyber methods which Leckner reported on in 2018. This was preventable had GDIT escalated Leckner's zero-day cyber reports up the chain-of-command at the EPA, as required in GDIT's contract. GDIT and Apex purposely retaliated against Leckner instead.

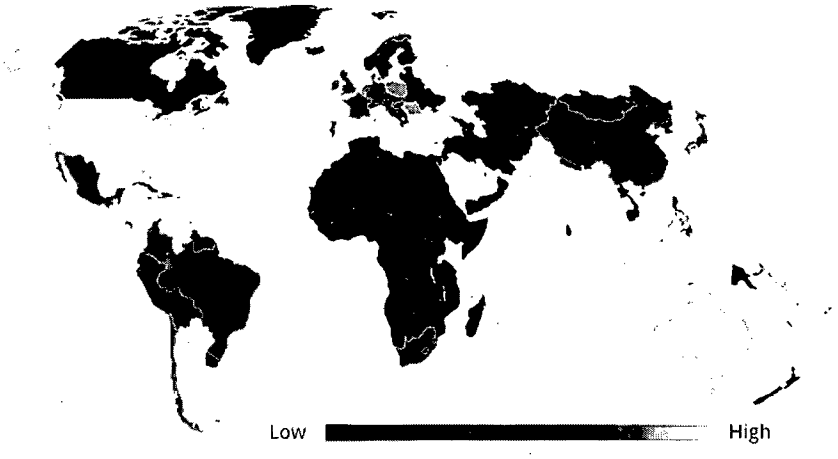

Figure 1: Log4j Security Breaches:
Flaw Challenges Global Security Leaders

Because the Log4j security flaw is so widespread and most organizations are unaware that they're impacted, an exploitation frenzy is currently underway in the cyber world. Security researchers have identified approximately 10 million Log4j exploitations attempts every hour in 2022. The retail industry is suffering the highest number of attacks, followed by technology services, financial services, manufacturing services, and federal and state government agencies across the globe.

Although Leckner's repeated cyber and fraud concerns were raised through official protected channels, the ALJ improperly concluded that "SOX whistleblower protection does not extend to cybersecurity risks." *See* ALJ Decision, p.12. Leckner reported that federal government information systems at federal agencies were at serious risk and were breached. GDIT knowingly

destroyed and altered evidence during official ALJ government proceedings.

On October 6, 2021, Deputy Attorney General Monaco launched the DOJ's Civil Cyber-Fraud Initiative[3] after flagging Leckner's False Claims Act ("FCA") complaint, to combat new and emerging cyber threats to the security of sensitive information and critical systems. This initiative encourages employees to assist the government in identifying violations and fraudulent conduct while protecting whistleblowers from retaliation.

"For too long, companies have chosen silence under the mistaken belief that it is less risky to hide a breach than to bring it forward and to report it," said Monaco. "Well that changes today. We are announcing today that we will use our civil enforcement tools to pursue companies, those who are government contractors who receive federal funds, when they fail to follow required cybersecurity standards — because we know that puts all of us at risk."

Monaco relied upon Leckner's outline of related allegations that the DOJ will now relentlessly pursue against federal contractors: knowingly providing deficient cybersecurity products and services; knowingly misrepresenting their cybersecurity practices and protocols; and knowingly violating obligations to monitor and report cybersecurity incidents and breaches.

These allegations were made by Leckner in his initial complaints, filed on May 31, 14 days before his discharge on June 13, 2018. OSHA even cited GDIT

---

[3] *See* https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative.

for violating government cybersecurity standards, practices, and protocols on information which Leckner reported prior to his retaliatory discharge which led to GDIT's decision to replace Leckner. Yet the ALJ failed to recognize that SOX whistleblower protection *does* extend to cybersecurity breaches and risks.

This petition is necessary to secure and maintain uniformity of this Court's decisions and the recent initiatives of the Department of Homeland Security, the Department of Justice, and the Securities Exchange Commission.

II

After Leckner's briefing at the certiorari stage, the SEC proposed a new set of rules and amendments that the SEC hopes will bolster the defense against cyber incidents. The SEC now aims to standardize disclosures of material cybersecurity incidents and improve visibility into a company's cybersecurity risk management and governance policies to better inform investors. The proposal covers cybersecurity incident disclosure and would amend Form 8-K to require a company to notify shareholders and the SEC when a material event such as a breach takes place within four days of material determination.

SOX already protects employees who disclose these activities. Employees have the right to complain about improperly installed software and mismanaged projects and systems because they indicate problems which may arise in the future, as they did in this case. Leckner disclosed serious material cybersecurity incidents and fraudulent billing activities to his supervisors and the EPA.

The EPA OIG in its initial investigation using randomly selected invoices uncovered overbilling practices of GDIT based on Leckner's complaints.[4] GDIT employees admitted to billing the EPA in their depositions for a contractual transition which they didn't perform, which resulted in over $200 million in emergency software being destroyed. GDIT defrauded the U.S. government and obstructed multiple federal investigations and will need to pay the United States back.

Even before the recent SEC proposal on cybersecurity, SOX mandates covered every single requirement that the SEC imposes on regulated industry, whether these requirements are reporting incidents, internal corporate structural requirements or provisions of the securities laws designed to ultimately protect shareholders. Every rule, regulation and law administered by the SEC is covered under SOX, not just laws related to the protection of shareholders.

If a company is negligent in failing to establish or maintain its internal controls on cybersecurity, that is a violation of its legal duties under SEC regulations. There is no public purpose that is served by allowing company managers to punish employees who raise concerns about management's neglect in failing to maintain required internal controls, even if no fraud is involved. Accord, *Smith v. Corning*, 496 F.Supp. 2d 244, 248 (W.D. NY 2007).

In *Klopfenstein v. PCC Flow Technologies Holdings, Inc.*, ARB Case No. 04-149, 2004-SOX-11 (May 31, 2006),

---

[4] *See* https://www.epa.gov/sites/default/files/2019-05/documents/_epaoig_20190520-19-p-0157.pdf.

the ARB addressed the scope of protected activity under SOX. At p.17, the ARB explained:

> SOX protection applies to the provision of information regarding not just fraud, but also "violation of . . . any rule or regulation of the Securities and Exchange Commission." 18 U.S.C. § 1514A(a)(1).

GDIT argued that the Leckner's communications were not protected. This argument is wrong. GDIT's entire business is predicated on compliance with the rules and regulations governing its practices. Not only are practices material to the company's stock prices, the entire corporate reputation and business plan is predicated on its reputation for demanding strict compliance with its practices.

III

The petition for certiorari presented similar questions as those recently settled in *United States ex rel. Brian Markus v. Aerojet Rocketdyne Holdings Inc., et al.*, Case No. 2:15-cv-02245-WBS-AC (E.D.Cal.), after the completion of Leckner's briefing stage, where the Department of Justice recognized violations of the whistleblower protection statutes.[5]

Aerojet recently agreed to pay $9 million to resolve allegations that it violated the False Claims Act by misrepresenting its compliance with cybersecurity requirements in certain federal government contracts, the Justice Department announced on July 8, 2022 after the petition for certiorari stage. The settlement resolves a lawsuit filed and litigated by former Aerojet

---

[5] *See* https://www.justice.gov/opa/pr/aerojet-rocketdyne-agrees-pay-9-million-resolve-false-claims-act-allegations-cybersecurity.

employee Markus against Aerojet under the qui tam or whistleblower provisions of the False Claims Act.

"Whistleblowers with inside information and technical expertise can provide crucial assistance in identifying knowing cybersecurity failures and misconduct," said Principal Deputy Assistant Attorney General Brian M. Boynton, head of the Justice Department's Civil Division. "The *qui tam* action brought by Mr. Markus is an example of how whistleblowers can contribute to civil enforcement of cybersecurity requirements through the False Claims Act," said U.S. Attorney Phillip Talbert.

Leckner and *Markus* overlap in key critical issues and both Leckner and Markus are considered whistleblowers. In light of *Markus*, the highest court of our nation should grant rehearing and the petition or this Court will be inconsistent with other federal cases on civil fraud and cybersecurity.

IV

The Government Accountability Office (GAO) recently rejected GDIT's bid protest of the Defense Information Systems Agency's (DISA) decision to award a mega contract to Leidos for a key Pentagon program. In February 2022, DISA issued a contract award worth up to $11.5 billion to Leidos. GDIT recently lost over $20 billion in contracts with the federal government where even DISA abruptly ended GDIT's milCloud 2.0 contract.

V

After the petition for certiorari stage, Peter Bermes, Attorney, Office of General Counsel, informed Leckner via email that the EPA's initial response to his Freedom

of Information Act requests withheld vital information. Specifically, information in a series of emails and attachments contained numerous redactions which proved that GDIT knew that Leckner had been blowing the whistle to the EPA and retaliation. GDIT recently since withdrawn its claims after being informed that Leckner is holding them accountable for damages for violating 18 U.S.C. § 1519 in another federal court. The EPA recently produced these documents in full with Exemption 4 redactions removed.

In violation of 18 U.S.C. § 1519, GDIT deliberately concealed evidence for FOIA requests submitted by Leckner during discovery where Leckner and his counsel sought records related to General Dynamics' unlawful activities in this matter.

VI

The Department withheld Leckner's first complaint filed on May 31, 2018, which never transferred over to the Fourth district. This was a violation of 18 U.S.C. § 1519, as the Department knowingly withheld and made false entries in the agency record, as Leckner reported this to the Office of the Secretary of Labor in 2019.

The agency also violated 29 C.F.R. § 1980.103, as the first complaints and dates of filing are required, by law, to be put on record by the Secretary. Even if the ALJ failed to put the evidence on record, the ALJ was required to put the initial complaints on record which were filed in the Ninth before case transfer. Leckner made telephonic and written complaints to OSHA and EPA starting on May 31, 2018. Leckner provided this evidence to Federal OSHA. Reference Petition Appendix I (the first "Complaint"); Appendix

IV (the "Date of Discharge"). The agency violated 29 C.F.R. § 1980.105(b), which states,

> [a]t the same time, the Assistant Secretary will file with the Administrative Law Judge a copy of the original complaint and a copy of the findings and/or order.

The agency also violated its *own* procedures with its Federal partner agencies. Reference Petition Appendix IV ("Coordination with Federal Partner Agencies"). The date the first complaint was filed with the EPA must be used as the complaint was filed within the whistleblower provision's filing period. Leckner filed his first complaint on May 31, fourteen days before his discharge on June 13, 2018. Reference Petition Appendix I (the "Complaint"); Appendix IV (the "Date of Discharge").

Furthermore, the respondents knowingly concealed evidence and misled the complainant regarding the retaliatory grounds for the adverse actions in such a way as to prevent him from knowing and discovering the requisite elements of a *prima facie* case.

In *Johnson v. Ry. Express Agency, Inc.*, 421 U.S. 454, 459-60, 95 S.Ct. 1716, 44 L.Ed.2d 295 (1975), the Supreme Court held that,

> Consistent with the common understanding that tolling entails a suspension rather than an extension of a period of limitations, petitioner is allowed whatever time remains under the applicable statute . . . .

The panel's erroneous holding affirming the Department's errors squarely conflicts with the Supreme

court's holding in *Johnson*. Leckner, however, timely filed his complaints.

VII

The petition for certiorari presented similar merits questions as those this Court resolved in *Department of Homeland Security v. MacLean*, 135 S.Ct. 913, 190 L.Ed.2d 771 (2015) where the Supreme Court recognized violations of the whistleblower protection statutes.

In *Department of Homeland Security v. MacLean*, the Supreme Court held that a federal air marshal was protected by the Whistleblower Protection Act when he leaked to the media an agency plan to stop air marshals from traveling due to a budget constraint. This was certainly a disclosure outside the chain of command. The Supreme Court held it was protected and MacLean was reinstated as an Air Marshal. In light of *MacLean*, this Court should grant the rehearing and the petition.

VIII

The petition for certiorari also presented similar merits questions as those this Court resolved in *Facebook Inc. v. Duguid*, 926 F.3d 1146 (9th Cir. April 1, 2021), explaining, that context is "a factor of considerable importance." The Supreme Court reversed, remanded, and explained this principle by saying, "where a sentence contains several antecedents and several consequents," courts should "read them distributively and apply the words to the subjects which, by context, they seem most properly to relate."

Here, without using Leckner's evidence, as the memory drive of evidence was misplaced by the Department, the ALJ erroneously concluded that Leckner's protected activity first began on April 13, by

taking one email out of *context* from the request for hearing which had emails in the request dating prior to April 13.

To be consistent with the Supreme Court's decision in *Facebook*, the Supreme Court should reverse, remand, and explain this principle by saying, "where an email thread contains several antecedents and several consequents, courts should read them distributively and apply the emails to the subjects and dates which, by context, they seem most properly to relate."

IX

The petition for certiorari presented the same merits questions and arguments as those the Department of Labor resolved in *Sylvester v. Parexel International LLC, ARB No. 07-123, ALJ Nos. 2007-SOX-039, 042*, *Munsey v. Federal Mine Safety and Health Review Comm'n*, 595 F.2d 735 (D.C. Cir. 1978), and *Passaic Valley Sewerage Comm. v. U.S. Department of Labor*, 992 F.2d 474, 478-79 (3rd Cir. 1993).

In *Sylvester*, the Board rejected the "definitively and specifically" standard and returned to the broad standard that better comports with the statute's remedial purpose. Not only was the "definitively and specifically" standard rejected, that standard undermined the purpose behind SOX. In *Munsey*, communications made through established channels-even those established informally by custom and usage, are near absolute and protected. In *Passaic Valley*, as long as an internal complaint made outside the formal reporting channels was made in good faith and not frivolous, it was protected.

CONCLUSION

For the foregoing reasons, the Petitioner asks this Court to grant this petition and reverse the flawed decision of the Ninth Circuit which affirmed the ALJ's decision and find that SOX whistleblower protection does extend to cybersecurity breaches and risks.

Respectfully submitted,

ERIK LECKNER
CYBERSECURITY EXPERT
PETITIONER PRO SE
747 S. MISSION ROAD
UNIT 2923
FALLBROOK, CA 92088
(760) 459-7772

JULY 22, 2022

RULE 44 CERTIFICATE

I, ERIK LECKNER, petitioner pro se, pursuant to 28 U.S.C. § 1746, declare under penalty of perjury that the following is true and correct:

1. This petition for rehearing is presented in good faith and not for delay.

2. The grounds of this petition are limited to intervening circumstances of a substantial or controlling effect or to other substantial grounds not previously presented.

/S/ ERIK LECKNER

Executed on July 22, 2022