

APPENDIX

INDEX TO APPENDICES

Opinion in the United States Court of Appeals for the Fourth Circuit (March 5, 2020)	App. 1
Order to Enter Final Judgment in the United States District Court for the Eastern District of Virginia Alexandria Division (June 22, 2018)	App. 27
Judgment in the United States District Court for the Eastern District of Virginia Alexandria Division (June 26, 2018)	App. 32
Order in the United States District Court for the Eastern District of Virginia Alexandria Division (June 18, 2018)	App. 33
Memorandum Opinion in the United States District Court for the Eastern District of Virginia Alexandria Division (April 16, 2018)	App. 34
Order in the United States District Court for the Eastern District of Virginia Alexandria Division (April 16, 2018)	App. 43
Order in the United States District Court for the Eastern District of Virginia Alexandria Division (September 18, 2017)	App. 44
Order Denying Petition for Rehearing and Rehearing en banc in the United States Court of Appeals for the Fourth Circuit (May 4, 2020)	App. 45
Order Entering Judgment of the Equal Employment Opportunity Commission (March 19, 2014)	App. 46
Order for Damages Evidence of the Equal Employment Opportunity Commission (January 13, 2014)	App. 68
Decision of the Equal Employment Commission (May 18, 2010)	App. 71

Recommended Decision of Administrative Judge Mark W. Harvey of the Department of Defense Office of Hearings and Appeals (September 5, 2007)	App. 82
Statutory, Regulatory, and Executive Order Provisions Involved	App. 94
ADEA	App. 94
Title VII	App. 100
Title 5 – Government Organization and Employees § 2302	App. 104
National Security Act of 1947.....	App. 110
DOD 5200.2-R	App. 117
Code of Federal Regulations Part 732 National Security Positions.....	App. 161
Executive Order 10450 Security requirements for Government employment.....	App. 163
Executive Order 12968 Access to Classified Information	App. 170
Executive Order 13292 Further Amendment to Executive Order 12958, as Amended, Classified National Security Information	App. 181

PUBLISHED**UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT**

No. 18-1890

WALTON CAMPBELL,

Plaintiff – Appellant,

v.

RYAN D. MCCARTHY, Secretary of the Army,

Defendant – Appellee.

Appeal from the United States District Court for the Eastern District of Virginia, at Alexandria. Claude M. Hilton, Senior District Judge. (1:17-cv-00568-CMH-TCB)

Argued: December 10, 2019

Decided: March 5, 2020

Before KING, AGEE, and RICHARDSON, Circuit Judges.

Vacated and remanded by published opinion. Judge King wrote the opinion, in which Judge Agee and Judge Richardson joined. Judge Richardson wrote a separate concurring opinion.

ARGUED: Nina Yuanyuan Ren, KALIJARVI, CHUZI, NEWMAN & FITCH, P.C., Washington, D.C., for Appellant. Sean Douglas Jansen, OFFICE OF THE UNITED STATES ATTORNEY, Norfolk, Virginia, for Appellee. **ON BRIEF:** Richard R. Renner, KALIJARVI, CHUZI, NEWMAN & FITCH, P.C., Washington, D.C., for Appellant. G. Zachary Terwilliger, United States Attorney, Lauren A. Wetzler, Chief, Civil Division, OFFICE OF THE UNITED STATES ATTORNEY, Alexandria, Virginia, for Appellee.

KING, Circuit Judge:

Plaintiff Walton Campbell, a civilian employee of the Army Corps of Engineers, initiated this civil action against the Secretary of the Army (the “Army”) challenging the Army’s decision to suspend him from his employment pending review of his security clearance.¹ In his operative complaint, Campbell alleges three claims: a claim under Title VII of the Civil Rights Act of 1964 (the “Title VII claim”), a claim under the Age Discrimination in Employment Act of 1967 (the “Age claim”), and a claim under the Whistleblower Protection Act of 1989 (the “Whistleblower claim”). After dismissing without prejudice the Whistleblower claim for failure to exhaust administrative remedies, the district court awarded summary judgment to the Army on the Title VII and Age claims. Shortly thereafter, the court denied Campbell’s motion to alter or amend judgment. Campbell has appealed and, as explained below, we are satisfied that the Supreme Court’s decision in *Department of the Navy v. Egan*, 484 U.S. 518 (1988), deprived the district court of jurisdiction to review any of Campbell’s claims. We therefore vacate and remand for dismissal.

¹ Campbell started these proceedings in the District of Columbia. After that district court granted the Army’s motion to transfer venue to the Eastern District of Virginia, Campbell filed his operative complaint in Alexandria. *See Campbell v. Speer*, No. 1:17-cv-00568 (D.D.C. May 17, 2017), ECF No. 11; *Campbell v. Speer*, No. 1:17-cv-00568 (E.D. Va. Jul. 7, 2017), ECF No. 28. Campbell therein sued the Acting Secretary of the Army in his official capacity. The Secretary of the Army in his official capacity has properly been substituted as the defendant. *See* ECF Nos. 3, 44.

I.

On July 27, 2004, Walton Campbell began working as a physical scientist at the Topographic Engineering Center, a laboratory of the Corps of Engineers’ Engineer Research and Development Center.² Located adjacent to Fort Belvoir in Alexandria, the Topographic Engineering Center develops “products that could improve the U.S. Army’s warfighting capabilities,” and physical scientists employed there must maintain a top secret security clearance with sensitive compartmented information access. *See* J.A. 127.³ Because of the classified nature of its work, the Topographic Engineering Center is a “restricted area” subject to prohibitions against recording and photographic devices in certain sections thereof. And many Topographic Engineering Center employees work in the Center’s Sensitive Compartmented Information Facility, in which recording and photographic devices are prohibited entirely.

A.

Within months of starting his job, Campbell became embroiled in a workplace dispute with three of his coworkers. Because the escalation of that dispute resulted in the suspension of Campbell’s employment pending review of his security clearance by the Army’s Central Clearance Facility, we first relate the circumstances of that dispute.

² The Topographic Engineering Center is now called the Army Geospatial Center.

³ Citations herein to “J.A. ___” refer to the contents of the Joint Appendix filed by the parties in this appeal. Because this appeal concerns an award of summary judgment, we recite the facts in the light most favorable to Campbell, as the non-moving party. *See United States v. Ancient Coin Collectors Guild*, 899 F.3d 295, 312 (4th Cir. 2018).

1.

When Campbell began working at the Topographic Engineering Center, he did not possess a security clearance. As a result, he was assigned duties unrelated to his physical scientist position while his security clearance application was processed. During that time, Campbell was assigned to work on the Source Acquisition Team. Campbell's first-level supervisor was then Mary Pat Santoro, the Chief of the Information Services Branch.

While he was assigned to the Source Acquisition Team, Campbell would regularly have lunch with three of his younger coworkers, Tish Kennan, Alana Hubbard, and Marty Downing. Kennan, Hubbard, and Downing wished, however, that Campbell would not socialize with them because his behavior made them uncomfortable. That was because, among other things, Campbell described himself as a person who often sought revenge and remarked that he knew how to construct bombs. Kennan, in particular, related that Campbell frequently paid her unwanted attention. Campbell would stare at her and refer to her as "Trouble." *See* J.A. 214. He also told Kennan that he had located information about her estranged husband on the internet and that he had driven through the neighborhood where she resided. On several occasions, Campbell had given Kennan unwanted gifts. For example, Campbell gave Kennan a battery cleaner after she commented that she needed to jump-start her car. And Campbell often followed Kennan around, "wait[ing] for [her] outside the bathroom" or "[standing] aside while [she] was having conversations with others so that he could follow [her] afterwards." *Id.* at 218.

On February 9, 2005, the Army granted Campbell a top secret security clearance with sensitive compartmented information access. Campbell's security clearance thus

authorized him to access information that, if released, would result in “exceptionally grave damage to national security.” *See* J.A. 196. That security clearance also allowed Campbell to access the Sensitive Compartmented Information Facility, and his workspace was relocated therein. In accepting his security clearance, Campbell agreed to abide by certain conditions. Relevant here, Campbell agreed to report any change in his legal residence within seven days.

2.

Thirteen days later, on February 22, 2005, Campbell was transferred from the Source Acquisition Team to the Current Operations Team. As a result of this transfer, Charles Lopez, the Chief of the Terrain Analysis Branch, became Campbell’s first-level supervisor. And although Campbell no longer worked with Kennan, Hubbard, or Downing, he continued to visit them in the Source Acquisition Team’s workspace and to involve himself in their lunch plans. By the end of that week, on February 25, 2005, Campbell had worn out his welcome. That day, without invitation, Campbell went to the Source Acquisition Team’s workspace and watched Kennan and Hubbard as they worked. At one point, R. Paul Harwig — a Division Chief of the Topographic Engineering Center and Campbell’s second-level supervisor — entered the workspace and observed Campbell “sitting too close” to Kennan and Hubbard. *See* J.A. 197. When Kennan and Hubbard left to go to lunch, Campbell followed them. Hubbard recalled that “because of his disturbing behavior,” they were too “scared” to tell Campbell that he was not welcome to join them for lunch. *Id.* at 216.

Following an unpleasant lunch outing to a Chili's restaurant, Kennan and Hubbard reported their concerns about Campbell's behavior to Division Chief Harwig. More specifically, they informed Harwig that they were planning to tell Campbell that "he could no longer go to lunch and that he could no longer follow [them] around [the Topographic Engineering Center], and that [they] did not want any more gifts from him." *See* J.A. 216-17. In response, Harwig asked the Current Operations Team Leader, Jeffrey Popp, to inform Campbell that he was no longer permitted in the Source Acquisition Team workspace, that he was not to distract Kennan and Hubbard from their work, and that he was to minimize his contacts with Kennan and Hubbard. Team Leader Popp relayed those instructions to Campbell on February 28, 2005.

3.

Shortly after meeting with Team Leader Popp, on March 7, 2005, Campbell sent an e-mail message entitled "Whistleblowing on aberrant staff behavior" to Topographic Engineering Center leadership, including Division Chief Harwig and Branch Chief Lopez. *See* J.A. 199-205. In that message and an accompanying attachment, Campbell denied any wrongdoing and made allegations concerning the "professionalism and mental stability of [Kennan and Hubbard], who hold current [sensitive compartmented information] clearances and have access to classified materials." *Id.* at 199. Regarding Kennan, Campbell claimed that her complaints about him were the result of a laundry list of "personal stresses." *Id.* at 199, 203-04. And Campbell painted Hubbard as a "disgruntled employee," who, during the lunch outing of February 25, 2005, complained "angr[ily] and openly" about having to train new employees (a complaint that Campbell surmised was

“unusual for a proud mother of two”) and used “vitriolic language” to describe her supervisor’s and a coworker’s professional competence. *Id.* Following an investigation into Campbell’s allegations, Harwig concluded that Campbell’s e-mail “was in retaliation as a result of having his feelings hurt and that his allegations [had] no merit.” *Id.* at 208.

On the evening of March 9, 2005, after learning of Campbell’s allegations against her, Kennan reported to Branch Chief Santoro that Campbell’s behavior made her feel unsafe at work. And Kennan explained to Santoro that she no longer felt safe outside of work because Campbell had tried to follow her home from the Topographic Engineering Center that afternoon. Kennan related that, as she was driving home, she saw Campbell pull into traffic behind her. Believing that Campbell was following her, Kennan “purposefully made a series of turns to evade him” and returned to the Topographic Engineering Center to make her report to Santoro. *See J.A. 209.*

Division Chief Harwig and Branch Chief Lopez met with Campbell on March 10, 2005, and informed him that he was under investigation for misconduct related to his interactions with Kennan and Hubbard. On that occasion, Campbell was instructed to avoid all contact with Kennan and Hubbard and to relocate his workspace from the Sensitive Compartmented Information Facility to a less-restricted section of the Topographic Engineering Center. On the next day, March 11, 2005, Harwig, Lopez, Team Leader Popp, and the Topographic Engineering Center Chief of Security, Thomas Cain, met with Campbell regarding Kennan’s stalking allegations. That meeting was held in a room of the Topographic Engineering Center in which information classified as secret may

be discussed. After the meeting, Campbell remained in the room while potentially classified information was discussed.

During the weekend, in addition to relating her stalking allegations to Branch Chief Santoro, Kennan obtained from a Fairfax County magistrate an emergency protective order against Campbell, which resulted in the issuance of an arrest warrant for stalking.⁴ When Fairfax County police officers sought to execute that warrant using the legal residence that Campbell had reported to the Topographic Engineering Center, they discovered that it was a post-office box address. Because the officers were unable to locate Campbell's residence, the Fort Belvoir Military Police and Security Chief Cain detained Campbell upon his arrival at work on Monday, March 14, 2005. Campbell was searched by the Fairfax County police officers when they arrived to execute the arrest warrant. The search revealed that Campbell was wearing a microcassette recorder with a microphone that was wired from the recorder through his shirt sleeve to his wristwatch. The officers also recovered a cellphone with a camera, two additional driver's licenses in Campbell's name from Louisiana and Texas, a digital voice recorder, and a pen that appeared to contain a recording device (but that was actually an FM radio).

Believing that Campbell's possession of the recording devices posed a national security threat, the Army Criminal Investigation Command and the FBI were notified. FBI Special Agents interviewed Campbell, and Campbell explained that he intended to record

⁴ On October 19, 2005, Campbell was tried on the stalking charge in a Fairfax County court. The jury found Campbell not guilty.

his conversations with Kennan so that he would have proof if she threatened him. Campbell also admitted that he attempted to record the March 11, 2005, meeting in order to protect himself from Kennan's stalking accusations. The FBI Agents concluded that, although Campbell had committed a security violation, he had not managed to compromise any classified information.

B.

Contemporaneously, the Director of the Topographic Engineering Center and Campbell's third-level supervisor, Robert Burkhardt, notified the Commanding Officer of the Engineer Research and Development Center, Colonel James Rowan, of Campbell's stalking arrest and his possession of the recording devices and out-of-state driver's licenses. Director Burkhardt also informed Colonel Rowan that Campbell had provided a post-office box address as his legal residence. Based on that information, Rowan determined that Campbell "posed a risk to national security" and suspended Campbell's access to classified information. *See* J.A. 123, 243. Rowan subsequently recommended that the Central Clearance Facility permanently revoke Campbell's security clearance. That recommendation was predicated on Rowan's conclusion that revocation was "in the interests of national security" because of Campbell's "potential criminal conduct, personal conduct and inappropriate use of photography equipment and recording devices in a restricted area." *Id.* at 191, 245. Before making the recommendation regarding Campbell, Rowan had never recommended a permanent revocation of an Engineer Research and

Development Center employee's security clearance. On April 4, 2005, Campbell was notified that his security clearance had been suspended.⁵

By memorandum of April 27, 2005, Division Chief Harwig notified Campbell of his proposal to suspend Campbell from his employment with the Army pending review of his security clearance by the Central Clearance Facility. This proposed suspension was based on Campbell's provisional loss of his security clearance, plus the requirement of Campbell's position that he maintain a security clearance. And the memorandum further specified why Campbell's security clearance had been suspended:

1. "Violation of security regulations or practices whereby [Campbell] brought recording devices, both voice and image into a secure facility on multiple occasions." *See* J.A. 188.
2. "Acts of commission that indicate poor judgment, unreliability or untrustworthiness whereby [Campbell] covertly recorded conversation with [his] supervisors." *Id.*
3. "Knowingly misrepresenting [his] current legal residence to [his] supervisor, Mr. Chuck Lopez." *Id.*
4. "Acts of commission that indicate poor judgment, unreliability or untrustworthiness whereby [Campbell] created a disturbance in the workplace involving co-workers." *Id.*

On May 19, 2005, Campbell, with counsel, submitted an oral reply to Director Burkhardt, who was responsible for deciding whether to adopt Division Chief Harwig's proposal to suspend Campbell from his employment. Campbell did not dispute that his security clearance was suspended for the reasons articulated in Harwig's memorandum.

⁵ We refer herein to Campbell's access to classified information and his security clearance collectively as his "security clearance."

Rather, Campbell argued that he should be reassigned to unclassified duties while the Central Clearance Facility reviewed his security clearance. Nonetheless, based on the reasons that Campbell's security clearance was suspended, Burkhardt determined that Campbell's actions were distinguishable from other Engineer Research and Development Center employees who had lost access to classified information but were reassigned to unclassified duties. Amplifying Harwig's statement of the reasons that Campbell's security clearance was suspended, Burkhardt explained:

1. “On 14 March 05, [Campbell] entered a restricted facility, namely the [Topographic Engineering Center], wearing a recording microphone on [his] wrist that was connected via a wire through [his] sleeve to a micro cassette recorder in [his] pants pocket. On that date, [he] secretly recorded conversations inside the restricted facility.” *See* J.A. 229.
2. “On 14 March 05, [Campbell] entered a restricted facility, namely the [Topographic Engineering Center], bringing with [him] a digital voice recorder, and a cell phone camera with capabilities for both still images and video.” *Id.* at 230.
3. “On 14 March 05, [Campbell] admitted to an FBI Special Agent that [he] ‘had recorded another conversation with [his] supervisors.’ [Campbell’s] supervisors [reported] that that conversation took place on 11 March 2005 in room 506, which is a classified area. They [also reported] that [Campbell] remained in room 506 after that conversation while another conversation took place in which classified material was discussed. . . . Because [Campbell] wore a wire on two separate dates, [he] intentionally disregarded national security regulations and policies, and *showed a willingness to compromise classified information* for the sake of [his] own, personal interests.” *Id.* (emphasis added).
4. “Instead of providing [his] current [legal] residence, [Campbell] provided a post office box number at a commercial mail facility.” *Id.*
5. “[Campbell] created a disturbance in the workplace involving coworkers. Specifically, [Campbell] boasted to co-workers that [he

was] a person who sought revenge and knew how to make bombs. [Campbell's] boast created fear and apprehension on the part of [his] co-workers, and such fear and apprehension stifles open and timely discussion and reporting of suspicious or unusual activity, which could have a significant impact on the mission and on National Security.” *Id.*

In short, Burkhardt determined that Campbell’s actions resulting in the suspension of his security clearance were distinguishable from those of the Engineer Research and Development Center employees who were reassigned to unclassified duties because Campbell had taken “overt action that could have compromised classified information.”

See J.A. 229. Namely, Campbell brought recording and photographic devices to the Topographic Engineering Center and attempted to record conversations therein, misrepresented his legal residence, and made his coworkers feel unsafe. Burkhardt further related that “[t]he Commander of the [Engineer Research and Development Center] ha[d] never recommended that any clearance be revoked, until [Campbell’s] case. In all cases, not one of the employees took any overt action that could have compromised classified information.” *Id.* For those reasons — that is, the reasons why Campbell’s security clearance had been suspended — Burkhardt concluded that “[u]nder the circumstances, [Campbell’s] retention in duty status would be detrimental to national security interests.” *Id.* at 231. Burkhardt thus suspended Campbell’s employment with the Army pending review of his security clearance.

C.

Twelve years later, in early 2017, following lengthy administrative proceedings before the Department of Defense Office of Hearings and Appeals and the Equal

Employment Opportunity Commission (the “EEOC”), Campbell commenced this civil action against the Army.⁶ Campbell alleges that the Army discriminated and retaliated against him when it declined to reassign him to unclassified duties and instead suspended him pending review of his security clearance. Those allegations underlie the three claims of his operative complaint, that is, the Title VII claim, the Age claim, and the Whistleblower claim.

Pursuant to Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6), the Army moved in July 2017 to dismiss Campbell’s operative complaint for lack of subject matter jurisdiction and for failure to state a claim. Especially pertinent here, the Army argued that the Supreme Court’s decision in *Department of the Navy v. Egan*, 484 U.S. 518 (1988), deprived the district court of jurisdiction to review any of Campbell’s claims. The Army also maintained that judicial review of the Whistleblower claim was foreclosed by Campbell’s failure to exhaust administrative remedies and that he had failed to sufficiently state claims of discrimination or retaliation.

On September 18, 2017, after argument of the motion to dismiss, the district court declined to dismiss the Title VII and Age claims, concluding that it was “of the opinion that [Campbell had] stated claims upon which recovery may be had.” *See Campbell v. Speer*, No. 1:17-cv-00568, slip op. at 1 (E.D. Va. Sept. 18, 2017), ECF No. 41. And the

⁶ The proceedings before the Department of Defense Office of Hearings and Appeals resulted in the restoration of Campbell’s security clearance on September 26, 2007. Notwithstanding, on March 19, 2014, an EEOC administrative judge found in favor of the Army. The EEOC proceedings concluded on December 2, 2016, when the administrative judge’s decision was affirmed by the Office of Federal Operations.

court dismissed without prejudice the Whistleblower claim because Campbell had “not exhausted his administrative remedies.” *Id.* The court did not, however, address the Army’s argument that, under *Egan*, it lacked subject matter jurisdiction to review any of Campbell’s claims.

Thereafter, for reasons explained in its Opinion of April 16, 2018, the district court awarded summary judgment to the Army on the Title VII and Age claims. Although the Army again argued that review of any of Campbell’s claims was foreclosed by *Egan*, the court failed to address that contention. Reaching the merits of Campbell’s claims, the court ruled that Campbell could not establish a *prima facie* case of either sex or age discrimination, that the Army had “provided legitimate, non-discriminatory reasons for the suspension decision, and [that Campbell could not] demonstrate that those reasons were pretextual.” *See Campbell v. Speer*, No. 1:17-cv-00568, slip op. at 6-7 (E.D. Va. Apr. 16, 2018), ECF No. 65. The court also ruled that Campbell could not establish a *prima facie* case of retaliation and that he had “not produced evidence to show that [the Army’s] justifications [for the suspension were] pretextual.” *Id.* at 8-9. Subsequently, the court denied Campbell’s motion to alter or amend judgment. This appeal followed, and we possess jurisdiction under 28 U.S.C. § 1291.⁷

⁷ Our jurisdiction extends to the Whistleblower claim even though the district court dismissed that claim without prejudice. Of course, “[t]he jurisdiction of a court of appeals is generally limited to the review of final decisions made by the district courts, within the meaning of 28 U.S.C. § 1291, and to the review of certain interlocutory orders, as provided for in 28 U.S.C. § 1292.” *See Williamson v. Stirling*, 912 F.3d 154, 169 (4th Cir. 2018). And a dismissal without prejudice is generally not an appealable final order. *See De’Lonta v. Johnson*, 708 F.3d 520, 523 n.2 (4th Cir. 2013). Nevertheless, when “the grounds of the (Continued)

II.

We review *de novo* a district court’s dismissal of a complaint for lack of subject matter jurisdiction. *See Doe v. Meron*, 929 F.3d 153, 163 (4th Cir. 2019). We also review *de novo* a district court’s award of summary judgment. *See United States v. Ancient Coin Collectors Guild*, 899 F.3d 295, 312 (4th Cir. 2018). In this appeal, however, because the Army maintains that the district court lacked subject matter jurisdiction to review any of Campbell’s claims, we are obliged to first address the question of jurisdiction. *See Sigmon Coal Co. v. Apfel*, 226 F.3d 291, 299 (4th Cir. 2000), *aff’d sub nom. Barnhart v. Sigmon Coal Co.*, 534 U.S. 438 (2002); *Goldsmith v. Mayor & City Council of Balt.*, 845 F.2d 61, 64 (4th Cir. 1988).

III.

In *Department of the Navy v. Egan*, a civilian Navy employee with a criminal record and history of alcohol abuse was denied a security clearance. *See* 484 U.S. 518, 521-22 (1988). He accordingly became ineligible for his Navy position. *Id.* After the Merit Systems Protection Board concluded that it lacked authority to review the Navy’s security clearance decision, the employee appealed. *Id.* at 522-25. Emphasizing that classifying

dismissal make clear that no amendment could cure the defects in the plaintiff’s case,” a dismissal order is “final in fact and therefore appealable.” *See Goode v. Cent. Va. Legal Aid Soc’y, Inc.*, 807 F.3d 619, 623 (4th Cir. 2015) (internal quotation marks omitted). Here, Campbell could not cure his failure to exhaust administrative remedies for the Whistleblower claim by amending his complaint. Accordingly, the Order dismissing the Whistleblower claim without prejudice is a final appealable decision. We thus possess jurisdiction to review the court’s dismissal of that claim pursuant to § 1291.

and controlling access to “information bearing on national security” is the province of the Executive, the Supreme Court recognized that “the protection of classified information must be committed to the broad discretion of the agency responsible,” including the “broad discretion to determine who may have access to it.” *Id.* at 527, 529. To that end, the Court reasoned that the “[p]redictive judgment” required of security clearance decisions was best left to “those with the necessary expertise in protecting classified information.” *Id.* at 529. The Court thus agreed that, absent specific authorization from Congress (and there was none), the Merit Systems Protection Board did not possess the authority to review the reasons underlying a security clearance decision. *Id.* at 530.

We have adhered to the view that *Egan* generally proscribes judicial review of a security clearance decision “absent a specific mandate from Congress providing otherwise.” *See Hegab v. Long*, 716 F.3d 790, 794 (4th Cir. 2013); *Reinbold v. Evers*, 187 F.3d 348, 357-58 (4th Cir. 1999); *Becerra v. Dalton*, 94 F.3d 145, 148-49 (4th Cir. 1996); *Guillot v. Garrett*, 970 F.2d 1320, 1324-25 (4th Cir. 1992); *see also Jamil v. Sec'y, Dep't of Def.*, 910 F.2d 1203, 1205-06 (4th Cir. 1990) (extending *Egan* to judicial review of security clearance decisions). And we have never discerned an “unmistakable expression of purpose by Congress in Title VII [of the Civil Rights Act of 1964]” to subject security clearance decisions “to judicial scrutiny.” *See Becerra*, 94 F.3d at 149.⁸ But we have not

⁸ Several of our sister circuits have also concluded that, under *Egan*, security clearance decisions cannot be reviewed for violations of Title VII. *See, e.g., Ryan v. Reno*, 168 F.3d 520, 523-24 (D.C. Cir. 1999); *Brazil v. U.S. Dep't of the Navy*, 66 F.3d 193, 196-97 (9th Cir. 1995).

had occasion to consider whether Congress has provided for judicial review of security clearance decisions through the Age Discrimination in Employment Act of 1967 (the “ADEA”) or the Whistleblower Protection Act of 1989 (the “WPA”). As explained below, Congress has not specifically provided for any such review in either statute.

A.

We first consider the ADEA. And, as it must, our inquiry begins with the plain language thereof. *See Stewart v. Iancu*, 912 F.3d 693, 702 (4th Cir. 2019). After all, Congress’ intent generally will be most apparent “from the words of the statute itself.” *See Sigmon Coal Co. v. Apfel*, 226 F.3d 291, 304 (4th Cir. 2000), *aff’d sub nom. Barnhart v. Sigmon Coal Co.*, 534 U.S. 438 (2002). “To determine a statute’s plain meaning, we not only look to the language itself, but also the specific context in which the language is used, and the broader context of the statute as a whole.” *See Hately v. Watts*, 917 F.3d 770, 784 (4th Cir. 2019) (internal quotation marks omitted).

As codified at 29 U.S.C. § 633a, the federal-sector provision of the ADEA prohibits age discrimination against federal employees. *See* 29 U.S.C. § 633a. Specifically, § 633a provides that “[a]ll personnel actions” involving federal employees “who are at least 40 years of age . . . shall be made free from any discrimination based on age.” *Id.* § 633a(a). To that end, the EEOC “is authorized to enforce” § 633a(a) “through appropriate remedies, including reinstatement or hiring of employees with or without backpay.” *Id.* § 633a(b). Section 633a further authorizes “[a]ny person aggrieved” to “bring a civil action” for “such legal or equitable relief as will effectuate the purposes” thereof. *Id.* § 633a(c). “[B]y its terms,” § 633a thus “does not confer broad authority” on the federal courts to review

security clearance decisions. *See Egan*, 484 U.S. at 530. That is, nothing in § 633a plainly “evidence[s] the kind of unmistakable expression of purpose,” *see Becerra*, 94 F.3d at 149 (quoting *Guillot*, 970 F.2d at 1325), that *Egan* requires in order to subject a security clearance decision to review by “an outside nonexpert body” such as a federal court, *see Egan*, 484 U.S. at 529.

Our confidence that Congress did not provide for judicial review of security clearance decisions through the ADEA is bolstered by § 633a’s legislative history. Though we generally “need look no further” if the plain language of the statute is unambiguous, *see Hately*, 917 F.3d at 784, mirroring the Supreme Court’s approach in *Egan*, we will consider § 633a’s “language along with . . . its legislative history,” *see Egan*, 484 U.S. at 530 (internal quotation marks omitted). We do so to confirm that Congress did not otherwise express its intent to subject security clearance decisions to judicial review for violations of § 633a. *See King v. Burwell*, 135 S. Ct. 2480, 2496 (2015) (recognizing that courts must “take care not to undo what [Congress] has done”); *In re Sunterra Corp.*, 361 F.3d 257, 265 (4th Cir. 2004) (recognizing that when plain meaning conflicts with “clearly expressed” congressional intent, a court may look beyond unambiguous statutory language (internal quotation marks omitted)).

Like the legislative history for the ADEA’s private-sector provisions, the legislative history for § 633a indicates that Congress was primarily concerned with “remov[ing] discriminatory barriers against employment of older workers.” *See* S. Rep. No. 93-690, at 56 (1974); H.R. Rep. No. 93-913, at 40-41 (1974); *see also* S. Rep. No. 90-723, at 7 (1967) (“It is not the purpose of [the ADEA’s private-sector provisions] to require the employment

of anyone, regardless of age, who is not qualified on grounds other than age to perform the job. . . . The purpose of this legislation, simply stated, is to insure that age, within the limits prescribed herein, is not a determining factor in a refusal to hire.”); H.R. Rep. No. 90-805, at 6 (1967) (explaining that the “primary objective” of the ADEA’s private-sector provisions is “the promotion of employment opportunities for older workers”). Indeed, Congress appears to have considered § 633a’s applicability to government personnel actions taken in the interests of national security and declined to disturb the discretion of the Executive with respect to such actions. When submitting the Conference Report for the Fair Labor Standards Amendments of 1974, Pub. L. No. 93-259, 88 Stat. 55 (1974), which set forth § 633a, the Bill’s sponsor explained:

Questions have been raised about the applicability of the Age Discrimination provisions to the discretion which now may rest in the heads of certain executive agencies to terminate an employee in the interests of the national security of the United States. It was not the intent of the conferees to affect the exercise of such discretion, other than by barring actions which, in fact, would be illegal, such as a termination of employment or a refusal to hire based on age.

See 120 Cong. Rec. 8,764 (1974).⁹ We are thus satisfied that there is no “unmistakable expression of purpose by Congress” in § 633a of the ADEA to authorize judicial review of security clearance decisions. *See Becerra*, 94 F.3d at 149; *Guillot*, 970 F.2d at 1325.

⁹ In determining legislative intent, the statements of a bill’s sponsor made during debate are “entitled to weight.” *See Lewis v. United States*, 445 U.S. 55, 63 (1980).

B.

Next, we turn to the WPA. And, again, our inquiry begins with the plain language of the statute. *See Stewart*, 912 F.3d at 702. As codified at 5 U.S.C. § 2302, the WPA proscribes “personnel action” taken in retaliation for certain whistleblowing activities. Those activities include (1) the disclosure of information evidencing violations of “any law, rule, or regulation” or “gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety” and (2) “the exercise of any appeal, complaint, or grievance right granted by any law, rule, or regulation.” *See* 5 U.S.C. §§ 2302(b)(8), (9)(A). And § 2302(a)(2)(A) of Title 5 identifies twelve types of prohibited personnel actions. Only one of those personnel actions — that is, “any other significant change in duties, responsibilities, or working conditions” — could conceivably cover a security clearance decision. *Id.* § 2302(a)(2)(A)(xii).

Arguably, a security clearance decision could result in “a significant change in duties, responsibilities, or working conditions,” by rendering a federal employee ineligible for her position. *See* 5 U.S.C. § 2302(a)(2)(A)(xii). But *Egan* requires an “unmistakable expression of purpose by Congress” to subject a security clearance decision to judicial scrutiny. *See Becerra*, 94 F.3d at 149; *Guillot*, 970 F.2d at 1325. We thus cannot conclude that “by its terms,” the WPA specifically “confer[s] broad authority . . . to review a security-clearance determination.” *See Egan*, 484 U.S. at 530; *Hesse v. Dep’t of State*, 217 F.3d 1372, 1378 (Fed. Cir. 2000) (concluding that § 2302(a)(2)(A)(xii) “falls far short of constituting a specific statement of congressional intent to authorize review of security clearance determinations”); *see also SKY CABLE, LLC v. DIRECTV, INC.*, 886 F.3d 375,

388 (4th Cir. 2018) (recognizing that “*ejusdem generis* instructs that, when general words follow the enumeration of specific items in a list, the general words apply only to other items akin to those specifically enumerated” (internal quotation marks omitted)).

Likewise, our examination of the relevant legislative history — in particular that of the Whistleblower Protection Enhancement Act of 2012 (the “WPEA”), Pub. L. No. 112-199, 126 Stat. 1465 (2012) — fortifies our conclusion that Congress did not intend to provide for judicial review of security clearance decisions through the WPA. The legislative history for the WPEA — which strengthened whistleblower protections, in part by amending the WPA — reflects that Congress explicitly recognized a “critical need” to extend “the protections for whistleblowers to include those who are retaliated against through the loss of their security clearances or access to classified information.” *See* S. Rep. No. 112-155, at 35-36 (2012) (citing *Hesse*). And although Congress appears to have considered providing for review of retaliatory security clearance decisions by both the Merit Systems Protection Board and the federal courts, the Senate Homeland Security and Governmental Affairs Committee Report accompanying the 2012 Act explained “that an Executive Branch process can provide adequate review of security clearance retaliation.” *Id.* at 36, 39. For the reasons specified therein, the Act did not “provide for any judicial review of security clearance retaliation claims” by whistleblowers in the WPA, or elsewhere. *Id.* at 40.¹⁰ Therefore, we are similarly satisfied that there is no “unmistakable

¹⁰ The WPEA as enacted did not contain any provision extending whistleblower protections to security clearance decisions. *See* Pub. L. No. 112-199, 126 Stat. 1465 (2012); *see also Gulf Oil Corp. v. Copp Paving Co.*, 419 U.S. 186, 200 (1974) (observing (Continued)

expression of purpose by Congress” in the WPA to subject security clearance decisions to judicial review. *See Becerra*, 94 F.3d at 149; *Guillot*, 970 F.2d at 1325.

C.

Because Title VII, the ADEA, and the WPA do not specifically provide for judicial review of a security clearance decision, we must evaluate whether any of Campbell’s three claims against the Army can be assessed without reviewing the suspension of his security clearance. And we are readily satisfied that they cannot. As a result, *Egan* deprived the district court of subject matter jurisdiction in this litigation.

Under *Egan*, a claim that an adverse employment decision violated a plaintiff’s statutory rights is unreviewable when it “necessarily depends upon a review of” an agency’s security clearance decision. *See Guillot*, 970 F.2d at 1326. In other words, when review of such a claim requires review of “the very issue[] that the Supreme Court has held [is] non-reviewable” — namely, a security clearance decision — *Egan* deprives the federal courts of subject matter jurisdiction. *See Becerra*, 94 F.3d at 149.

that the deletion of language from the statute as enacted “strongly militates against a judgment that Congress intended a result that it expressly declined to enact”). A similar provision that also committed review of certain agencies’ retaliatory security clearance decisions to the Executive was later enacted as part of the Intelligence Authorization Act for Fiscal Year 2014. *See* Pub. L. No. 113-126, 128 Stat. 1390, 1417-20 (2014).

Campbell argues that Director Burkhardt’s conclusion that Campbell posed a unique threat to national security and thus could not be reassigned to unclassified duties was simply a pretext for discrimination and retaliation.¹¹ But Campbell’s security clearance was suspended for the same reasons relied on by Burkhardt to reach that conclusion. Under the burden-shifting framework upon which Campbell’s Title VII and Age claims rely, determining whether the reasons for suspending Campbell were legitimate and non-pretextual thus requires review of the Army’s security clearance decision. *See McDonnell Douglas Corp. v. Green*, 411 U.S. 792, 807 (1973); *Ryan v. Reno*, 168 F.3d 520, 523-24 (D.C. Cir. 1999); *Brazil v. U.S. Dep’t of the Navy*, 66 F.3d 193, 196-97 (9th Cir. 1995). Therefore, the district court lacked subject matter jurisdiction with respect to the Title VII and Age claims. So too with the Whistleblower claim, which requires reviewing the Army’s security clearance decision to determine whether Campbell was suspended for engaging in some protected activity rather than for the reasons he provisionally lost his security clearance. *See Bonds v. Leavitt*, 629 F.3d 369, 381 (4th Cir. 2011) (setting forth requirements for claim of WPA retaliation).

Seeking to clear this jurisdictional hurdle, Campbell emphasizes the Supreme Court’s conclusion in *Egan* that, under 5 U.S.C. § 7513, the Merit Systems Protection Board has jurisdiction to review “adverse actions” to determine “whether transfer to a

¹¹ During oral argument of this appeal, Campbell’s primary assertion was that he was “entitled to reasonable inferences” that Director Burkhardt’s conclusion that he “posed a unique threat” and thus could not be reassigned to unclassified duties was “pretextual.” *See* Oral Argument at 1:10-1:20, *Campbell v. Esper*, No. 18-1890 (4th Cir. Dec. 10, 2019), <http://www.ca4.uscourts.gov/oral-argument/listen-to-oral-arguments>.

nonsensitive position was feasible.” *See Egan*, 484 U.S. at 530. Accordingly, Campbell maintains that jurisdiction to review his claims — each of which concern Director Burkhardt’s refusal to reassign him to unclassified duties — is unaffected by *Egan*. He is mistaken in that regard.

Contrary to Campbell’s assertion, *Egan* does not “impose on an agency the obligation, independent of statute or regulation, to transfer employees who lose their security clearance.” *See Jamil*, 910 F.2d at 1208. Rather, when an “independent source for a right to a transfer [to a nonsensitive position] exists,” *Egan* authorizes a limited review of whether such a transfer is feasible. *Id.* at 1208-09; *Guillot*, 970 F.2d at 1326-27. Campbell argues that, in this case, such a review is enabled by the prior instances in which Engineer Research and Development Center employees who lost their access to classified information were reassigned to unclassified duties. But nothing in this record refutes Director Burkhardt’s determination that the Engineer Research and Development Center’s past practice was inapposite to Campbell. As with Burkhardt’s ultimate conclusion that Campbell’s “retention in duty status would be detrimental to national security interests,” that determination was predicated on the reasons that Campbell’s security clearance was suspended. *See* J.A. 229-31. We do not see how, in these circumstances, the Engineer Research and Development Center’s past practice provides an “independent source for a right to a transfer” as contemplated by *Egan* and our precedents. *See Jamil*, 910 F.2d at 1208-09; *Guillot*, 970 F.2d at 1326-27.

* * *

In sum, Campbell was suspended by the Army pending review of his security clearance for the very same reasons that he provisionally lost his security clearance. Because review of any of Campbell’s claims requires review of the suspension of his security clearance — a review that necessarily “goes to the very heart of the protection of classified information” — *Egan* deprived the district court of subject matter jurisdiction to review each of Campbell’s claims. *See Becerra*, 94 F.3d at 149. The court thus erred by failing to dismiss these claims outright for lack of subject matter jurisdiction.

IV.

Pursuant to the foregoing, we vacate the district court’s judgment and remand for dismissal of the operative complaint for want of subject matter jurisdiction.

VACATED AND REMANDED

RICHARDSON, Circuit Judge, concurring:

I readily join the majority's fine opinion in full. But I write separately to note the Supreme Court's odd use of legislative history in this context. It is hard to fathom how we might unearth within legislative history 'a specific mandate from Congress' or 'an unmistakable expression of purpose' to overcome the presumption against review of security-clearance decisions made by the executive branch. The "psychoanalysis of Congress" is a "weird endeavor" in any event, *United States v. Public Utilities Commission of California*, 345 U.S. 295, 319 (1953) (Jackson, J., concurring), but particularly so when the sensitivity and importance of a discretionary executive branch action requires that we avoid review in the first place. But the Supreme Court has instructed that we try. *Department of the Navy v. Egan*, 484 U.S. 518, 530 (1988). And so we do.

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

WALTON CAMPBELL,
Plaintiff,

v.

MARK ESPER,
Secretary of the Army,
Defendant

Case No. 1:17-cv-568-CMH-TCB

**DEFENDANT'S MEMORANDUM IN SUPPORT OF UNOPPOSED MOTION
REQUESTING ENTRY OF FINAL JUDGMENT**

Pursuant to Federal Rule of Civil Procedure 58(d), Defendant, Mark Esper, Secretary of the Army (“Army”), respectfully requests that the Court enter final judgment as a separate document. In support of this request, the Army states as follows:

1. Federal Rule of Civil Procedure 58(b)(1)(C) provides that the “clerk must . . . enter judgment when . . . the court denies all relief.”
2. On March 16, 2018, the Army filed a Motion for Summary Judgment requesting that the Court dismiss all of Plaintiff’s remaining claims. ECF No. 57.
3. On April 16, 2018, after the Army’s Motion for Summary Judgment was fully briefed, the Court issued an Order and Opinion granting the Army’s Motion for Summary Judgment and dismissed all of Plaintiff’s remaining claims. ECF Nos. 65-66.
4. On May 11, 2018, Plaintiff filed a Motion to Alter or Amend Judgment requesting that the Court reconsider its grant of the Army’s Motion for Summary Judgment. ECF Nos. 67-68.

*So Ordered
Claude M. Hilton
VS DG
June 22, 2018*

5. On June 18, 2018, after Plaintiff's Motion to Alter or Amend Judgment was fully briefed, the Court issued an Order denying Plaintiff's Motion to Alter or Amend Judgment. ECF No. 72.

Accordingly, because the Court has denied all relief requested by Plaintiff, the Army respectfully requests that the Court enter final judgment as a separate document pursuant to Federal Rule of Civil Procedure 58. Although Plaintiff does not agree with the Court's Order and Opinion granting the Army's Motion for Summary Judgment, Plaintiff does not oppose the Army's request that the Court enter judgment as a separate document.

Respectfully submitted,

G. ZACHARY TERWILLIGER
UNITED STATES ATTORNEY

Lauren A. Wetzler,
Chief, Civil Division

By: /s/ Sean D. Jansen
Sean D. Jansen
Assistant U.S. Attorney
Virginia State Bar No. 82252
Counsel for Defendant
Office of the United States Attorney
101 W. Main Street, Suite 8000
Norfolk, Virginia 23510
Phone: (757) 441-6331
Fax: (757) 441-6689
Email: sean.jansen@usdoj.gov

CERTIFICATE OF SERVICE

I hereby certify that on June 21, 2018, I filed the foregoing with the Clerk of Court using the CM/ECF system, which will send a notification of electronic filing (NEF) to the following counsel of record:

Sarah Martin, Esq.
Nina Ren, Esq.
Richard R. Renner, Esq.
Kalijarvi, Chuzy & Newman & Fitch, P.C.
818 Connecticut Avenue, N.W., Suite 1000
Washington, D.C. 20006
smartin@kcnlaw.com
nren@kcnlaw.com
rrenner@kcnlaw.com

By: /s/
Sean D. Jansen
Assistant U.S. Attorney
Virginia State Bar No. 82252
Counsel for Defendant
Office of the United States Attorney
101 W. Main Street, Suite 8000
Norfolk, Virginia 23510
Phone: (757) 441-6331
Fax: (757) 441-6689
Email: sean.jansen@usdoj.gov

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

WALTON CAMPBELL,

Plaintiff,

v.

Case No. 1:17-cv-568-CMH-TCB

MARK ESPER,
Secretary of the Army,

Defendant

**DEFENDANT'S UNOPPOSED MOTION REQUESTING ENTRY OF FINAL
JUDGMENT**

Pursuant to Federal Rule of Civil Procedure 58(d), Defendant, Mark Esper, Secretary of the Army, hereby respectfully files this Motion Requesting Entry of Final Judgment. The grounds for this motion are fully set forth in the concurrently-filed memorandum in support of the motion.

Respectfully submitted,

G. ZACHARY TERWILLIGER
UNITED STATES ATTORNEY

Lauren A. Wetzler,
Chief, Civil Division

By: /s/ Sean D. Jansen
Sean D. Jansen
Assistant U.S. Attorney
Virginia State Bar No. 82252
Counsel for Defendant
Office of the United States Attorney
101 W. Main Street, Suite 8000
Norfolk, Virginia 23510
Phone: (757) 441-6331
Fax: (757) 441-6689
Email: sean.jansen@usdoj.gov

CERTIFICATE OF SERVICE

I hereby certify that on June 21, 2018, I filed the foregoing with the Clerk of Court using the CM/ECF system, which will send a notification of electronic filing (NEF) to the following counsel of record:

Sarah Martin, Esq.
Nina Ren, Esq.
Richard R. Renner, Esq.
Kalijarvi, Chuzy & Newman & Fitch, P.C.
818 Connecticut Avenue, N.W., Suite 1000
Washington, D.C. 20006
smartin@kcnlaw.com
nren@kcnlaw.com
rrenner@kcnlaw.com

By: /s/
Sean D. Jansen
Assistant U.S. Attorney
Virginia State Bar No. 82252
Counsel for Defendant
Office of the United States Attorney
101 W. Main Street, Suite 8000
Norfolk, Virginia 23510
Phone: (757) 441-6331
Fax: (757) 441-6689
Email: sean.jansen@usdoj.gov

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA**

Alexandria Division

Walton Campbell)
)
 Plaintiff,)
)
 v.) Civil Action No. 1:17-cv-568 (CMH-TCB)
)
)
)
 Mark Esper)
 Secretary of the Army)
)
 Defendant.)

JUDGMENT

Pursuant to the order of this Court entered on June 22, 2018 and in accordance with
Federal Rules of Civil Procedure 58, JUDGMENT is hereby entered in favor of the defendant
Mark Esper, Secretary of the Army and against the Plaintiff, Walton Campbell.

FERNANDO GALINDO, CLERK OF COURT

By: _____ /s/
Anitra Chastine
Deputy Clerk

Dated: June 26, 2018
Alexandria, Virginia

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA

Alexandria Division

WALTON CAMPBELL,)
Plaintiff,)
v.) Civil Action No. 1:17-cv-00568
MARK ESPER,)
Secretary of the Army)
Defendant.)

ORDER

THIS MATTER comes before the Court on Plaintiff's Motion to Alter or Amend this Court's April 16, 2018 Order. The Court is of the opinion that its previous Order was correct for the reasons stated. Accordingly, it is hereby

ORDERED that Plaintiff's Motion to Alter or Amend Judgment is DENIED.

Claude M. Hilton
CLAUDE M. HILTON
UNITED STATES DISTRICT JUDGE

Alexandria, Virginia
June 18, 2018

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA

Alexandria Division

WALTON CAMPBELL,)
Plaintiff,)
v.) Civil Action No. 1:17-cv-00568
MARK ESPER,)
Secretary of the Army)
Defendant.)

Memorandum Opinion

THIS MATTER comes before the Court on Defendant's Motion for Summary Judgment.

This suit arises out of the 852-day unpaid suspension that Plaintiff Walton Campbell, 57 years-old at the time of the suspension, was placed on by his employer, the Army Corps of Engineer's Engineer Research and Development Center (the "ERDC"). Beginning in 2004, Plaintiff was employed by the ERDC as a physical scientist at the ERDC's Topographic Engineering Center (the "TEC") laboratory in Alexandria, Virginia. Because the TEC laboratory is designated as a restricted area, and because the TEC works almost exclusively with classified information, Plaintiff was required to maintain a Top Secret clearance and access to Sensitive Compartmented Information.

Beginning in February 2005, Plaintiff's direct supervisor, Mr. Harwig, began to receive troubling reports from two of Plaintiff's coworkers, Ms. Kennan and Ms. Hubbard, regarding Plaintiff's behavior. On one instance the two women, both of whom Plaintiff alleges to be less than 40-years-old, described to Mr. Harwig behavior which "sounded to Mr. Harwig like stalking." When Plaintiff's access to a particular part of the TEC facility was removed and his interactions with the two women minimized following this report, Plaintiff complained to his supervisor and others about the coworkers' professionalism and mental stability, making several allegations against the coworkers. Mr. Harwig ultimately concluded that Plaintiff's allegations were unfounded.

Following this, Ms. Kennan reported that she felt unsafe around Plaintiff, and that "Plaintiff had previously commented that he was a person who sought revenge, knew how to make bombs, and that he had put chemicals in a former coworker's drink to give that person diarrhea." Ms. Kennan also alleged that Plaintiff had attempted to follow her home.

Plaintiff was placed under investigation for misconduct, and informed that he should avoid all contact with Ms. Kennan and Ms. Hubbard. Plaintiff alleges that he reported to Mr. Harwig that he felt threatened by Ms. Kennan and Ms. Hubbard due to their apparent false accusations against him, and that he

feared for his safety around Ms. Kennan because she had stated on multiple occasions that she was "a former Marine, a marksman and a good shot." According to Plaintiff, Mr. Harwig dismissed Plaintiff's concerns without investigation.

Soon after this, Plaintiff was detained and interviewed by Fort Belvoir Police for allegedly violating a restraining order that Ms. Kennan had taken out against him. The officers found that Plaintiff was wearing a recording device with a microphone wired through his shirt sleeve, and he was also in possession of a digital voice recorder and camera phone with video capabilities. Plaintiff was then interviewed by the FBI, during which he admitted to wearing the microphone in an attempt to record conversations with his coworkers, and admitted that on a prior occasion he had attempted to record a conversation with his supervisors.

Following these events, Plaintiff's access to classified materials was suspended. TEC Director Mr. Burkhardt made a preliminary decision to place Plaintiff on administrative suspension, without pay, pending the outcome of his security review, but offered Plaintiff an opportunity to rebut the allegations being made against him first. At a meeting on May 19, 2005, between Plaintiff, Burkhardt, and Plaintiff's attorney, Plaintiff did not dispute that he wore a recording device into a restricted facility on two previous occasions,

possessed numerous recording devices in a restricted facility, or that he commented about having the ability to make bombs or about how he was a person who took revenge. At that same meeting, Plaintiff's attorney warned Mr. Burkhardt that the Army could face an EEO action if Plaintiff was suspended without pay.

After the May 19 meeting, Mr. Burkhardt officially decided to suspend Plaintiff without pay pending adjudication of his security clearance, determining that retaining Plaintiff in a paid, duty status would be detrimental to national security interests. Mr. Burkhardt made this decision after speaking with Plaintiff's colleagues regarding the situation and reviewing documents pertinent to the allegations. Plaintiff remained on an indefinite, unpaid suspension for 852 days while the investigation was pending, from May 27, 2005, until his clearance was restored on September 26, 2007. In the interim, Plaintiff was found not guilty of the stalking charges after defending himself in a jury trial in Fairfax County. Plaintiff also filed a formal EEO complaint during this time, which ultimately resulted in a decision finding no discrimination on March 9, 2014. Plaintiff appealed the decision to the EEOC's Office of Federal Operations, which affirmed the decision on December 2, 2016.

Plaintiff filed suit on February 28, 2017, alleging that Defendant engaged in unlawful age and sex discrimination in

violation of Title VII of the Civil Rights Act and the Age Discrimination in Employment Act (the "ADEA") by placing Plaintiff on unpaid suspension rather than providing paid unclassified work for him during the adjudication of his security clearance. He also alleged retaliation in violation of Title VII and the ADEA due to Defendant's alleged refusal to consider and investigate Plaintiff's claims of age and sex discrimination that Plaintiff made before he was placed on indefinite suspension without pay.

Title VII provides that "[a]ll personnel actions" affecting federal employees like Plaintiff "shall be made free from any discrimination based on . . . sex." 42 U.S.C. § 2000e-16(a). Furthermore, the ADEA provides that "[a]ll personnel actions" affecting employees "who are at least 40 years of age . . . in executive agencies . . . shall be made free from any discrimination based on age." 29 U.S.C. § 633a(a). Under either statute, where a plaintiff does not present direct evidence of discrimination, he must prove a violation through the McDonnell Douglas burden-shifting framework. McDonnell Douglas Corp. v. Green, 411 U.S. 792 (1973). Under this framework, the plaintiff must first establish a *prima facie* case of discrimination or retaliation. Foster v. Univ. of Md. Eastern Shore, 787 F.3d 243, 250 (4th Cir. 2015). The burden then shifts to the employer to produce a legitimate, non-discriminatory reason for the

decision. Id. Finally, the plaintiff must establish that the employer's stated reason is merely a pretext. Reeves v. Sanderson Plumbing Prods., Inc., 530 U.S. 133, 142 (2000).

Here, Plaintiff cannot establish a *prima facie* case of either age or sex discrimination. To demonstrate a *prima facie* case of discrimination, a plaintiff must show that (1) he is a member of a protected class, (2) he suffered an adverse employment action, (3) at the time of the adverse action the plaintiff was performing at a level that met his employer's legitimate expectations, and (4) similarly situated employees outside of the plaintiff's protected class were treated more favorably. See Coleman v. Maryland Court of Appeals, 626 F.3d 187, 190 (4th Cir. 2010).

Although "plaintiffs are not required as a matter of law to point to a similarly situated comparator to succeed on a discrimination claim," where a plaintiff relies on comparators to establish his *prima facie* claim, those comparators must be "similar in all relevant respects," including "evidence that the employees dealt with the same supervisor" and "engaged in the same conduct without such differentiating or mitigating circumstances that would distinguish their conduct or the employer's treatment of them for it." Haywood v. Locke, 387 F. App'x 355, 359 (4th Cir. 2010).

Plaintiff attempts to identify similarly situated

comparators by pointing out that "all other employees whose clearances had not yet been approved, or had been suspended or revoked, had remained in paid duty status and assigned duties that did not require a security clearance." However, of the seventeen other ERDC employees who lost or were denied access to classified information, none are similarly situated. First, the decision maker in Plaintiff's case (Mr. Burkhardt) was not the decision maker in any of the other cases. Second, none of the other seventeen employees had their access to classified information suspended for even remotely similar reasons, and thus did not engage in the "same conduct" as Plaintiff.

Furthermore, even if Plaintiff could establish a *prima facie* claim of disparate treatment, Defendant has provided legitimate, non-discriminatory reasons for the suspension decision, and Plaintiff cannot demonstrate that those reasons were pretextual. Mr. Burkhardt explained in his decision letter that Plaintiff was placed on administrative leave because retaining Plaintiff in paid, duty status posed a danger to national security interests due to the multiple concerns regarding Plaintiff's alleged behavior. These justifications are supported by the evidence, and there is no evidence to show that they are merely pretextual. Thus, Plaintiff's discrimination claim fails as a matter of law.

Plaintiff's retaliation claim also fails as a matter of

law. Once again, under the McDonnell Douglas burden-shifting framework, Plaintiff must first establish a *prima facie* case of retaliation. To do so, Plaintiff must show that: (1) he engaged in a protected activity, (2) Defendant took an adverse action against him, and (3) there was a causal link between the protected activity and the adverse action. E.E.O.C. v. Navy Fed. Credit Union, 424 F.3d 397, 405-06 (4th Cir. 2005). To prove causation, a plaintiff claiming retaliation must show that reprisal was the "but for" cause of the personnel action. See Univ. of Tex. Sw. Med. Ctr. v. Nassar, 133 S. Ct. 2517, 2528 (2013) (applying "but for" standard of causation for retaliation claim under Title VII); Gross v. FBL Fin. Servs., Inc., 557 U.S. 167, 176-77 (2009) (applying same standard for retaliation claim under the ADEA).

Plaintiff cannot prove a *prima facie* case of retaliation because he cannot establish that "but for" a retaliatory motive, he would not have been suspended without pay. Plaintiff's alleged protected activity was his complaint at the May 19, 2005 meeting that he was subjected to disparate treatment and that he would bring an EEO action if Mr. Burkhardt did not retain Plaintiff in a paid position performing non-classified work. However, prior to this meeting, Mr. Burkhardt had already preliminarily determined that he was going to suspend Plaintiff without pay unless Plaintiff satisfactorily rebutted the

allegations made against him. Plaintiff did not do so when given the opportunity. Thus, Mr. Burkhardt had already made the decision to suspend Plaintiff before Plaintiff engaged in protected activity, and so Plaintiff cannot show that his protected activity was the "but-for" cause of his suspension.

Furthermore, as discussed *supra*, Defendant has put forward legitimate, non-discriminatory and non-retaliatory justifications for the suspension decision which are supported by the evidence, and Plaintiff has not produced evidence to show that those justifications are pretextual. Therefore, Plaintiff's retaliation claim fails as a matter of law.

For the foregoing reasons, this Court finds that Defendant is entitled to summary judgment. An appropriate order shall issue.


CLAUDE M. HILTON
UNITED STATES DISTRICT JUDGE

Alexandria, Virginia
April 16, 2018

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA

Alexandria Division

WALTON CAMPBELL,)
Plaintiff,)
v.) Civil Action No. 1:17-cv-00568
MARK ESPER,)
Secretary of the Army)
Defendant.)

ORDER

In accordance with the accompanying Memorandum Opinion, it is hereby

ORDERED that Defendant's Motion for Summary Judgment is GRANTED, and this case is dismissed.

Claude M. Hilton
CLAUDE M. HILTON
UNITED STATES DISTRICT JUDGE

Alexandria, Virginia
April 16, 2018

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA

Alexandria Division

WALTON CAMPBELL,)
Plaintiff,)
v.) Civil Action No. 1:17-cv-00568
ROBERT M. SPEER,)
Defendant.)

ORDER

THIS MATTER comes before the Court on Defendant's Motion to Dismiss for Lack of Jurisdiction and Motion for Judgment on the Pleadings. With regard to Counts I and II of the Amended Complaint, the Court is of the opinion that Plaintiff has stated claims upon which recovery may be had. With regard to Count III, the Court is of the opinion that Plaintiff has not exhausted his administrative remedies. Accordingly, it is hereby

ORDERED that Plaintiff's Motion to Dismiss is DENIED as to Counts I and II and GRANTED as to Count III, and Count III is dismissed without prejudice.

Claude M. Hilton
CLAUDE M. HILTON
UNITED STATES DISTRICT JUDGE

Alexandria, Virginia
September 18, 2017

FILED: May 4, 2020

UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

No. 18-1890
(1:17-cv-00568-CMH-TCB)

WALTON CAMPBELL

Plaintiff - Appellant

v.

RYAN D. MCCARTHY, Secretary of the Army

Defendant - Appellee

O R D E R

The court denies the petition for rehearing and rehearing en banc. No judge requested a poll under Fed. R. App. P. 35 on the petition for rehearing en banc.

Entered at the direction of the panel: Judge King, Judge Agee, and Judge Richardson.

For the Court

/s/ Patricia S. Connor, Clerk

**EQUAL EMPLOYMENT OPPORTUNITY COMMISSION
WASHINGTON FIELD OFFICE
131 M Street, N.E., Suite 4NW02F
Washington, D.C. 20507**

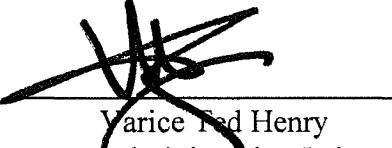
Walton B. Campbell,) EEOC No. 570-2006-00375X
Complainant,) Agency No. ACEERDC05JUL0922
)
)
v.)
)
)
John McHugh,)
Secretary,)
Department Of Army,)
Agency.)
)
)
)
)
) Date: March 19, 2014

ORDER ENTERING JUDGMENT

For the reasons set forth in the enclosed Decision judgment in the above-captioned matter is hereby entered. A Notice to the Parties explaining their appeal rights is attached to the Decision.

For timeliness purposes it shall be presumed that the parties received the foregoing Decision within five (5) business days after the date they were sent via first class mail.

It is so ORDERED.


Varice F. Henry
Administrative Judge
(202) 419-0717
(202) 419-0740

To:

Walton B. Campbell
6036 Richmond Highway
#211
Alexandria, VA 22303

June D.W. Kalijarvi, Esq.
Kalijarvi, Chuzi & Newman, PC
1901 L Street, NW, Ste. 610
WDC 20036

Timothy Felker, Esq.
Servicing Labor Counsel
U.S. Army Engineer Research & Development Center
CEERD-OC-A, Bldg. 2592
7701 Telegraph Road
Alexandria, VA 22315-3864

Linda S. Wilkinson, EEO Mgr.
ERDC-Army Corps of Engineers
Waterway Experiment Station
3909 Halls Ferry Road
Vicksburg, MS 39180-6199

U.S. EQUAL EMPLOYMENT OPPORTUNITY COMMISSION
Washington Field Office
131 M Street, N.E., Suite 04NW
Washington, D.C. 20507

Walton B. Campbell, Complainant,) EEOC No. 570-2006-00375X
) Agency No. ACEERDC05JUL0922
)
v.)
)
John McHugh, Secretary, Department Of Army, Agency.)
)
)
)
)
) Date: March 19, 2014

DECISION

This Decision is issued pursuant to 29 C.F.R. § 1614.109(g) (2013). This office issued an Acknowledgment Order on June 27, 2006. The Agency filed its Motion for Summary Judgment on November 2, 2006 (Agency Motion). Complainant filed a Response to the Agency's Motion on December 4, 2006. (Complainant's Motion). The Agency submitted its Reply to Complainant's Motion on December 18, 2006. (Agency Reply). Complainant submitted Complainant's Supplemental Clarification on January 2, 2007. (Complainant's Clarification). The Agency submitted its Response to Complainant's Clarification on January 9, 2007 (Agency Response). On September 19, 2007, this Judge issued a decision without a hearing in favor of the Agency.

Complainant timely filed an appeal with the EEOC's Office of Federal Operations (OFO) arguing that there were genuine issues of fact in dispute regarding the Agency's reasons for suspending him which were material to whether or not the suspension was discriminatory (or retaliatory). OFO agreed with Complainant's position and on May 14, 2010, issued a Decision reversing the AJ's decision (OFO Remand) without a hearing and the Agency's final order, and remanding the matter to the Washington Field Office Hearings Unit for the holding of a hearing.

A hearing was held before this Administrative Judge on December 3, 4, and 5, 2012. Eleven witnesses testified, including two called by Complainant, and nine called by both parties. One witness, R. Paul Harwig, the former Division Director of the Operations Division at the Agency had retired by the time of the hearing and failed to appear although called by both parties. His deposition was introduced pursuant to F. R. Civ. P. 32(a). CE Complainant's Exhibit (CE) 33. At the conclusion of the hearing the AJ directed the parties to file Closing Briefs on the

substantive issue of discrimination and retaliation and liability, and on the issue of the relevance of the Defense Office of Hearings and Appeals (DOHA) Recommended Decision and the Personnel Security Appeals Board (PSAB) decision reinstating Complainant's clearance. The AJ bifurcated the liability phase of the hearing and the damages phase. On January 13, 2014, an Order for Damages Evidence was sent to the parties.¹

ISSUE

The issue is whether the Agency discriminated against Complainant because of his of sex (male), age (57, D.O.B: 6/30/47) and/or retaliation/reprisal in violation of Title VII of the Civil Rights Act of 1964 (Title VII), 42 USC § 2000e-16, and the Age Discrimination in Employment Act (ADEA), 29 USC 633a when on May 27, 2005, Complainant was indefinitely suspended without pay pending determination of his secret security clearance.²

Report of Investigation (ROI) at C-2.

FACTUAL BACKGROUND

The Complainant is Dr. Walton Campbell. The Agency is the Department of the Army, Army Corps of Engineers, Engineer Research and Development Center (ERDC), Topographic Engineering Center (TEC), Operations Division. Complainant began his employment with the Agency on July 27, 2004, as a DB-1301-04 (GS-14 equivalent) Physical Scientist assigned to the Engineer Research and Development Center (ERDC), Topographic Engineering Center (TEC), Operations Division (Agency). HT at 47-48.

After Complainant entered on duty at the Agency it assigned him to the Information Services Branch, Source Acquisition Team (SAT) within the Operations Division, TEC, ERDC. Mary Pat Santoro (female) was the Branch Chief and Theresa Rasmussen (female) was the Team Leader. HT at 20. The other members of the SAT were two younger white females, Tish Kennan and Alana Hubbard, Marty Downing (male), and Loretta Williams (black female). HT at 51-52. Complainant, Ms. Kennan, Ms. Hubbard and Mr. Downing were all assigned to the SAT doing similar work although Ms. Kennan, Ms. Hubbard and Mr. Downing had TS/SCI clearances and worked in the Agency's SCIF to which Complainant was not allowed access. HT at 51-52; 368-370; 414-415, 418; ROI FFC Tr. at 67-68. The Division Chief of the Operations Division was R. Paul Harwig (male, age: 48, D.O.B.: 9/1/57); the Director of the TEC was Robert

¹That Order indicated that I believed Complainant to be the prevailing party in this case and required the parties to submit motions regarding the appropriate damages for this case. However, after a careful and arduous review of the hearings transcript, all of the evidence therein and all of the hearings record, I find that determination to have been premature. As such, the Agency need not reply.

²There is also an issue regarding the admissibility, relevance and governance of DOHA's Recommended Decision (CE 35) and the PSAB Decision (CE 36) restoring Complainant's security clearance (TS/SCI), which was originally raised by Complainant in his Prehearing brief and reasserted in his Post Hearing brief. This issue will be addressed in the Analysis section of this Decision.

Burkhardt (male, age: 57, D.O.B.: 10/26/48); and the Commanding Officer of the ERDC was Colonel James Rowan. ROI Exhibit (Ex.) F-1 at 57;³ HT at 253.

Personnel employed by the Agency in the Operations Division, TEC, ERDC are required to have security clearances which are called "Top Secret/Sensitive Compartmented Information (TS/SCI)." ROI Ex. F-15 at 128. Such personnel are subject to the provisions of Army Regulation (AR) 380-67 "Personnel Security Program." ROI Ex. F-15. When new personnel entered on duty in the Operations Division and TEC who did not have an appropriate clearance, the Agency applied for them to be granted a TS/SCI clearance. HT at 415; HT at 55-56; CE 33 at 18. In the interim the new employees were assigned unclassified duties to work on in an unclassified work space. *Id.* Employees of the Operations Division with TS/SCI clearances worked in a separate restricted facility called a SCIF (Secure Compartmentalized Intelligence Facility). HT at 370.

From July 27, 2004, until February 9, 2005, Complainant was assigned unclassified duties, that is, duties which did not require a security clearance, pending the Agency issuing him a TS/SCI security clearance, and he worked in an unclassified work space that did not require a clearance. HT at 48-49; 216; 369; ROI FFC Tr. at 17-18, 32. In September, 2004, Complainant received an interim Secret clearance; however, he continued to perform unclassified duties which did not require a clearance and he continued to work in an unclassified space. HT at 48-50; 214-215.

On February 9, 2005, Complainant was granted a TS/SCI clearance. AE 1. Enclosures (Encl.) 2,3. At that point Complainant was allowed access to the SCIF and Ms. Hubbard began to train Complainant in the SCIF. HT at 368-370; 418. On February 22, 2005, Complainant was transferred to the Current Operations Team, Terrain Analysis Branch, within the Operations Division, TEC, ERDC. HT at 19; 67-68. Charles Lopez was the Branch Chief of the Terrain Analysis Branch and Jeffrey Popp was the Team Leader of the Current Operations Team. *Id.* After Complainant was transferred to Mr. Lopez's Branch his assignments and duties did not require access to classified information. ROI Ex. F-8 at 84-85.

Between July 27, 2004, and March 7, 2005, Complainant's supervisors did not witness any performance or conduct by Complainant which caused them any concerns nor did they contemporaneously document any concerns and/or consider Complainant a threat to national security. HT at 30-32; 199, 210-211, 216, 217; 416-417, 421. Complainant's relationships with his coworkers and superiors were collegial and cordial and no one expressed any concerns about his conduct in the workplace. HT at 53-54, 118. All his supervisors in both branches and on both teams observed Complainant to be a good, professional, thorough and efficient worker ("a great

³The reference to ROI page numbers refers to the handwritten page numbers at the bottom center of the pages in the ROI. The reference to ROI Fact Finding Conference Transcript (ROI FFC Tr.) page numbers refers to the printed page numbers at the top right corner of the printed transcript. CE refers to Complainant's Exhibits. AE refers to Agency's Exhibits.

worker") who treated his supervisors and co-workers professionally and with respect. ROI FFC Tr. at 194; HT at 27, 30-3; 419.

From July 27, 2004, until February 25, 2005, Complainant regularly would have lunch with several of his co-workers on the SAT, including the two younger females on the Source Acquisition Team, Tish Kennan and Alana Hubbard, as well as Marty Downing. HT at 53. On several occasions Ms. Kennan would remark during these gatherings that she was a former Marine, a good marksman and that she knew how to shoot. HT at 59-61; 207. Occasionally during this period (July 27, 2004, - February 25, 2005) Ms. Hubbard and Ms. Kennan discussed with each other, Mr. Downing and their supervisors that they would prefer not to have Complainant accompany them to lunch but they did not want to tell him so for fear of hurting his feelings. HT at 398-399; 418; AE 1 Encls. 10, 16.

They also alleged Complainant followed Ms. Kennan around the work site. HT at 113-116; 212-213; 406. At no time during this time period did Ms. Kennan nor Ms. Hubbard advise anyone that they were afraid of Complainant or feared for their safety and no one observed Complainant behaving in a threatening manner toward anyone or behaving in a manner which caused anyone concern. HT at 30; 199, 210-211; 401-402; 416-417; ROI FFC Tr. at 138. Neither Ms. Kennan nor Ms. Hubbard ever told Complainant that they did not want him to socialize with them or that they were afraid of him; that he was sexually harassing, bothering/distracting them, interfering with their working or that he was inappropriately staring at Ms. Kennan. HT at 57-58.

Complainant was transferred within the Operations Division from Ms. Santoro's branch and Ms. Rasmussen's team to Mr. Lopez's branch and Mr. Popp's team effective February 22, 2005. AE 21. After his transfer to Mr. Popp's team and Mr. Lopez's branch Complainant was assigned unclassified duties and he worked in unclassified space "search[ing] the open literature for information on population densities of Iranian cities." HT at 67-68; 19-20.

On February 25, 2005, Complainant went to the SCIF in which Ms. Kerman and Ms. Hubbard were working and watched the program on which they were working. HT at 70-73. Shortly before Complainant, Ms. Hubbard and Ms. Kennan left the SCIF to go to lunch, Mr. Harwig, Division Director, Operations Division, opened the door to the SCIF and noticed Complainant observing Ms. Kennan and Ms. Hubbard work. *Id.* at 373-374. Mr. Harwig asked Complainant what he was doing in the SCIF and Complainant responded "observing." *Id.* Mr. Harwig responded "Oh" and left. *Id.* Ms. Hubbard, Ms. Kennan and Complainant then went to lunch at a public restaurant. *Id.* at 74-75.

The two younger women apparently went to the EEO office later that day and then told Mr. Harwig that Complainant had been "distracting" them and made them feel "uncomfortable." On February 25, 2005, Mr. Harwig had Complainant's access to the SCIF removed. CE 1. After February 25, 2005, Complainant had no further interaction with either Ms. Kennan or Ms. Hubbard. HT at 75-76.

Ms. Kennan and Ms. Hubbard also met contemporaneously with Mr. Popp and told him Complainant was "interfering" with their work and/or "bothering" or "distracting" them. HT at 22-25, 41. Mr. Popp told them he would speak to Complainant regarding their concerns - which he did. *Id.* at 23. Neither Ms. Kennan nor Ms. Hubbard told Mr. Popp that they were in fear of physical harm from Complainant nor did they claim he was sexually harassing one or both of them. *Id.* at 25. Neither Ms. Kennan nor Ms. Hubbard told Mr. Popp that Complainant touched them or said anything inappropriate to them or that he was too physically close to them, just that Complainant was interfering with their work. *Id.* at 41. Ms. Kennan and Ms. Hubbard indicated to Mr. Popp that they were concerned about their abilities to do their jobs. *Id.* at 32-33.

On February 28, 2005, Mr. Harwig directed Complainant's Team Leader, Mr. Popp, to direct Complainant not to distract or interact with either Ms. Kennan or Ms. Hubbard and to advise Complainant that his access to the SCIF had been removed. CEs 1, 2; HT at 26; AE 21. On March 1, 2005, Complainant's TS/SCI clearance was suspended by Mr. Harwig and he continued to be assigned unclassified duties. HT at 21.

On March 7, 2005, the Complainant responded to his supervisors when he sent an e-mail to his TEC chain of command, the TEC Legal Office, and TEC Security, entitled, "Whistleblowing on aberrant staff behavior," denying any misconduct and making allegations against Ms. Hubbard and Ms. Kennan that they were mentally unstable and unprofessional. AE 1 at 11-17. One of his allegations was that Tish Kennan was suffering from "malignant uterine cancer and a hysterectomy" and "being a single parent and having to commute every day across the Wilson Bridge." *Id.* at 16. Complainant alleged that these things, as well as some of the aforementioned comments at lunch gatherings made Ms. Hubbard and Ms. Kennan potential security risks. *Id.* at 11- 17; CE 3. According to Complainant, his security concerns arose from Ms. Kennan's and Ms. Hubbard's alleged loud and public derogatory comments and expressions of contempt for their supervisors. *Id.*; HT at 77-80; ROI FFC Tr. at 69-70.

On March 8, 2005, Mr. Harwig directed Complainant's Branch Chief, Mr. Lopez, to counsel Complainant concerning sexual harassment. ROI FFC Tr. at 60-61, 70-71; ROI Ex. F14. Also on March 8, 2005, Mr. Harwig interviewed Ms. Santoro, Ms. Rasmussen and Mr. Downing concerning Complainant's assertions concerning Ms. Kennan and Ms. Hubbard. CE 4. On March 9, 2005, Mr. Harwig interviewed Ms. Kennan and Ms. Hubbard concerning Complainant's assertions. CE 4; HT at 380-381. After all of the aforementioned consultations, Mr. Harwig concluded that Complainant's allegations against Ms. Kennan and Ms. Hubbard were without merit and need not be further investigated. CEs 5, 7. After Ms. Kerman and Ms. Hubbard learned on March 9, 2005, about Complainant's March 7, 2005, memorandum raising security concerns about them, they then told their supervisors they felt threatened by Complainant. HT at 379-380. On March 10, 2005, Mr. Harwig formally suspended Complainant's access to the Agency's secure facility (SCIF), advised Complainant he was being investigated for misconduct (re his alleged workplace behaviors) and again ordered Complainant not to interact with Ms. Kennan or Ms. Hubbard. CEs 4, 5; AE 21.

On March 11, 2005, Mr. Harwig and other Agency managers met with Complainant in Room 506 of the Cude Building concerning Ms. Kennan's allegations that Complainant had been "stalking" her and had followed her on her route home at the end of the day two days earlier, March 9, 2011. CE 7; HT at 94. Mr. Harwig indicated to Complainant that the allegations were viewed as a potential workplace violence issue and were considered serious. *Id.* Mr. Harwig asked Complainant about Ms. Kennan's allegation that he had stalked and/or followed her. Complainant denied the allegation and asserted that he in turn felt threatened by the two women. He advised Mr. Harwig that at the time that Kennan alleged that he had followed her, he had been at the gym with a co-worker (Laura Mulholland) and then had driven home. Mr. Harwig indicated that he thought there was a discrepancy in Complainant's statement regarding his address and instructed Mr. Lopez to ask Complainant what his current address was. *Id.*

Shortly after that meeting Mr. Lopez requested that Complainant provide them with his home address and telephone number. HT at 85-89. Mr. Lopez gave Complainant a form to complete with the requested information. ROI FFC Tr. at 184, 195. In his response Complainant provided the Agency his personal cell phone number and the address to which he was having his mail sent while he moved his place of residence. *Id.* Ms. Kennan on March 11, 2005, signed a Fairfax County arrest warrant accusing Complainant of stalking her two days earlier. *Id.* Mr. Harwig also asked Ms. Santoro, Ms. Rasmussen, Mr. Downing, Ms. Hubbard and Ms. Kennan to prepare statements about "incidents" involving Complainant. *Id.* at 14-15, 46-52.

After Complainant was apprised of Ms. Kennan's and Ms. Hubbard's allegations and after Mr. Harwig told Complainant that he was being investigated for misconduct, Complainant indicated that he brought a recording device to his unclassified work area. HT at 90-92; ROI FFC Tr. at 36-38, 42-43. On March 10, 11 and 14, 2005, Complainant unsuccessfully attempted to record conversations with his supervisors and/or co-workers.⁴ ROI FFC Tr. at 37-38; HT at 322-323.

On March 14, 2005, Complainant was confronted as he arrived at his unclassified work station, arrested and placed in handcuffs by Agency security personnel based on the warrant sworn out by Ms. Kennan. ROI Ex. F-8; CE 8. At the time of his arrest it was discovered that he had a recording device, a cell phone with photographic capability, and a "jogger's FM radio receiver." *Id.* After his arrest Complainant was interrogated by two FBI agents who determined that although they believed Complainant committed a security/procedural violation, he had not compromised any classified information despite having the recording device and the cell phone on his person and the FBI would therefore not conduct any further investigation. ROI Ex. F8 at 86-87; CE 8.

⁴The events at issue here occurred in and around a building on the Agency's premises next to Fort Belvoir, Virginia, designated as the Cude Building (Building 2592). A "Notice" is posted outside the Cude Building which states "Visitors" are "subject to inspection for firearms, explosives and dangerous weapons." ROI Ex. F-12 at 100. A sign outside Room 506 (an unclassified space) in the Cude Building states that: "Photographing, making notes, drawings, maps, or graphic representations of this area or its activities is prohibited." ROI Ex. F-11 at 97.

On March 14, 2005, the Agency formally removed Complainant's access to classified information. However, he continued to be assigned duties which did not require a security clearance. ROI Ex. F-8 at 84; HT at 21; 67-68. The Agency continued to assign Complainant unclassified duties to perform from March 14, 2005, until April 27, 2005, when he was placed on paid administrative leave until May 27, 2005, when he was placed on indefinite suspension without pay. *Id.* at 3. Complainant's supervisors confirmed that between March 14, 2005, and May 27, 2005, "[complainant's] current duties did not require for him to have access to classified information" and that he was performing his duties in an exemplary manner, proactively and thoroughly. *Id.*; ROI Ex. F-8; ROI FFC Tr. at 193-194.

On March 15, 2005, the County of Fairfax, Virginia charged the Complainant with "Stalking." AE 2 at 100. That information was a matter of public record and was considered reportable derogatory information under AR 380-67, paragraph 2-200. ROI at 77, 88; 119-200. Mr. Burkhardt was aware of this information and under the aforementioned guidance was allowed to consider it when making his determination to suspend Complainant. *Id.* Complainant was subsequently convicted by a Judge on the charge of stalking on June 27, 2005. CE 27 at 225-226. However, Complainant was later found not guilty of the same charge by a jury on October 19, 2005. CE 29 at 228. All references to this charge were ultimately ordered expunged from all official records.

On April 27, 2005, the Agency issued Complainant a Notice of Proposed Suspension (indefinite suspension without pay) pending adjudication of his security clearance. Complainant and his then-attorney presented an oral reply to the proposed indefinite suspension to the deciding official, Robert Burkhardt, on May 19, 2005. ROI at 70-72. In that oral reply Complainant raised the issue that he was being discriminated against with respect to the proposal to indefinitely suspend him without pay instead of assigning him unclassified duties and/or placing him in a position which did not require a security clearance.⁵ *Id.* at 71-72. Complainant emphasized that he believed he was being treated differently from his two young female co-workers, Ms. Kennan and Ms. Hubbard. On May 27, 2005, the Agency issued a decision placing Complainant on indefinite suspension without pay, specifically citing in its decision letter Complainant's allegations that he was being discriminated against, and stating that the Agency did not believe his EEO claims. ROI Exhibit F-5 at 71-72.

On November 16, 2005, Complainant advised Mr. Harwig and Mr. Lopez of the October 19, 2005, decision finding him not guilty of stalking. However, the Agency decided not to allow him to return to work at that time pending a final determination regarding his security clearance. Complainant remained on indefinite suspension without pay until the Agency restored his clearance effective September 26, 2007, after the DOD Office of Hearings and Appeals (DOHA) determined that Complainant's security clearance should be restored. The Department of the

⁵This oral reply to the Agency's Notice of Proposed Suspension in which he raised the issue of discriminatory disparate treatment is the basis of Complainant's allegation(s) of reprisal.

Army concurred and restored Complainant's clearance. HT at 119; CE 35, CE 36.

ANALYSIS

Absent direct evidence of discrimination, the complainant in a Title VII case must carry the initial burden under the statute of establishing a *prima facie* case of discrimination. The burden of establishing a *prima facie* case is not onerous. To establish a *prima facie* case of disparate treatment, a Complainant may demonstrate that he/she was treated less favorably than a similarly situated employee outside his/her protected group. *Furnco Constr. Corp. v. Waters*, 438 U.S. 567 (1978). Absent comparative data, Complainant may also establish a *prima facie* case by setting forth sufficient evidence to create an inference of discrimination. *Texas Dep't of Cnty. Affairs v. Burdine*, 450 U.S. 248, 256 (1981), n. 6; *McDonnell Douglas Corp. v. Green*, 411 U.S. 792, 802-03 (1973).

If Complainant establishes a *prima facie* case of discrimination, the burden then is on the Agency to articulate a legitimate, nondiscriminatory reason for its challenged actions. *Burdine*, 450 U.S. at 252-54; *McDonnell Douglas Corp.* 411 U.S. at 802. If the Agency does so, the *prima facie* inference drops from the case. *St. Mary's Honor Center v. Hicks*, 509 U.S. 502, 507, 510-11 (1993). Complainant then has to prove by a preponderance of the evidence that the proffered explanation is a pretext for unlawful discrimination. *Hicks*, 509 U.S. at 511; *Burdine*, 450 U.S. at 252-53; *McDonnell Douglas*, 411 U.S. at 804. Complainant always retains the ultimate burden of persuading the trier of fact that the Agency unlawfully discriminated against him/her. *Hicks*, 509 U.S. at 511; *United States Postal Service Bd. of Governors v. Aikens*, 460 U.S. 711, 715 (1983).

The *McDonnell Douglas* burden-shifting framework applies in reprisal cases. See *Hochstadt v. Worcester Foundation for Experimental Biology, Inc.*, 425 F.Supp. 318 (D. Mass. 1976), *aff'd*, 545 F.2d 222 (1st Cir. 1976); *McKenna v. Weinberger*, 729 F.2d 783 (D.C. Cir. 1984); *Downing v. U.S.P.S.*, EEOC Appeal No. 01822326 (September 19, 1983). Accordingly, a reprisal complainant must first establish a *prima facie* case by a preponderance of the evidence by showing that (1) the complainant engaged in protected activity; (2) the employer was aware of the protected activity; (3) the complainant was subsequently subjected to adverse treatment; and (4) the adverse action followed the protected activity within such a period of time that a retaliatory motivation may be inferred. See *Downing v. U.S.P.S.*, EEOC Appeal No. 01822326 (September 19, 1983). Thereafter, the standard *McDonnell Douglas* burden-shifting framework requires the Agency to articulate a legitimate, non-discriminatory reason for its actions, which reason the complainant is then required to show is a pretext for unlawful discrimination by the Agency. See *Burdine*, 450 U.S. at 253; *McDonnell Douglas*, 411 U.S. at 804; *Hicks*, 509 U.S. at 507-08.

DOHA and PSAB Decisions

In a decision dated September 5, 2007, an Administrative Judge of the Defense Office of Hearings and Appeals (DOHA) issued a "Recommended Decision" (DOHA Recommendation)

finding that it was consistent with the national interest for complainant's security clearance to be restored to him. CE 35. The Agency Personnel Security Appeals Board (PSAB) then issued a final determination accepting and ratifying the Administrative Judge's decision. CE 36.

On October 29, 2012, in his Prehearing Brief and again in his Closing Brief of February 28, 2013, Complainant argued that these decisions should not only be included in the hearings record, but should also be established as findings of fact as either admissions against interest by a party opponent pursuant to Rule 801(d)(2) of the Federal Rules of Evidence (FRE) and/or should collaterally estop the Agency from challenging them and the EEOC should adopt them as facts in this proceeding. On November 13, 2012, the Agency submitted its Motion in Opposition (Opposition Motion) to the arguments made in Complainant Prehearing Brief.

I find the Agency's arguments regarding this issue the more persuasive ones. In this case I must deny Complainant's motion because it is well established that the EEOC has no jurisdiction to review this or any security clearance decision of the Department of Defense. *Department of Navy v. Egan*, 484 U.S. 518, (Feb. 23, 1988). Complainant is petitioning the EEOC not only to review the security clearance decision, but to apply that decision in his own proceeding.

A long line of precedent limits the EEOC's review of cases involving denial (or revocation) of security clearance. *Sifflett v. National Security Agency*, 01910403. 2914/C10 (1991). However, while the EEOC is not permitted to review the merits of a security clearance decision, it can review such decisions to determine whether the security considerations were applied in a non-discriminatory manner. *Id., Chatlin v. Department of the Navy*, EEOC Request No. 05900188 (June 1, 1990).

This case concerns a matter of national security. The U.S. Supreme Court has "recognized the Government's 'compelling interest' in withholding national security information from unauthorized persons in the course of executive business." *Egan*, 484 U.S. at 527. The Court also found: "for 'reasons... too obvious to call for enlarged discussion, [citation omitted] the protection of classified information must be committed to the broad discretion of the agency responsible, and this must include broad discretion to determine who has access to it. Certainly, it is not reasonably possible for an outside nonexpert body to review the substance of such judgment and to decide whether the agency should have been able to make that necessary affirmative prediction with confidence." *Egan*, 484 U.S. at 529.

Additionally, Complainant's motion should be denied because OFO remanded the subject complaint with the finding that neither the decision to review his security clearance nor the outcome of the review is at issue here. (OFO Remand). Clearly the DOHA Recommendation meets this standard of exclusion as an outcome determinative decision after a review of his security clearance. The Agency correctly pointed out that Granting Complainant's motion would essentially preclude the Agency from contending that Complainant was a security risk as its articulated legitimate non-discriminatory reason for indefinitely suspending Complainant without

pay pending security clearance review while using as the basis an Administrative Judge's decision reviewing Complainant's security clearance. Complainant's request to have the DOHA Recommendation established as findings of fact is therefore hereby Denied.

FINDINGS

Assuming *arguendo* that Complainant has met the standards for a *prima facie* case of discrimination based on sex, age and reprisal, he has failed to demonstrate by a preponderance of the evidence that the Agency's articulated nondiscriminatory reasons for not allowing him to continue working while his security clearance was under review were a pretext for discrimination on the aforementioned alleged bases in violation of Title VII of the Civil Rights Act of 1964 (Title VII), 42 USC § 2000e-16, and the Age Discrimination in Employment Act (ADEA), 29 USC 633a.

The hearing testimony corroborates the Agency's position that it had legitimate, nondiscriminatory reasons for revoking his security clearance, e.g., Complainant had made comments in social settings with coworkers regarding his knowledge of bomb making, he entered a restricted area of the facility with a concealed recording device and attempted to (or possibly in fact did make) audio recordings⁶, he failed to provide an accurate current address when required to do so and he created through his behaviors a disturbance in the workplace involving a potential for workplace violence.

Paul Harwig, Complainant's second line supervisor provided more specific articulations of the aforementioned reasons in his recommendation memorandum to Mr. Burkhardt. He indicated that Dr. Campbell had shown a history and pattern of behavior that indicated poor judgment, unreliability and untrustworthiness.⁷ He specifically, listed the following:

- a. Violations of security regulations or practices whereby he brought recording devices, both voice and image into a secure facility on multiple occasions.
- b. Knowingly misrepresenting his current legal address to his supervisory chain of command.

⁶Complainant's argument at the hearing and the Fact Finding Conference in March of 2006 that he only "attempted" to make recordings is ultimately of no legal significance. ROI, FFC at 78-79. For national security purposes, an "attempted" recording, versus a "successful" recording is a distinction without a difference. Either scenario is sufficient to justify the Agency's determination that the Complainant was untrustworthy under AR 380-67, Chapter 2-200 of which refers to "acts of omission or commission that indicate poor judgment, unreliability or untrustworthiness." ROI at 119, chapter 2-200(i).

⁷While not specifically cited in the recommendation memorandum, the incidents and circumstances surrounding Complainant's alleged stalking behaviors, as well as his subsequent behavior(s) in response to those allegations, clearly influenced managements perceptions and opinions regarding his judgement, reliability and trustworthiness. They also comprise an important part of the events that occurred and ultimately lead to the revocation of Complainant's access to classified materials and his security clearance.

- c. Acts of commission that indicate poor judgment, unreliability or untrustworthiness where he has a history of making veiled threats about his ability to make explosive devices.
- d. Acts of commission that indicate poor judgment, unreliability or untrustworthiness where he recorded a conversation with his supervisors. AE 1 at pg.1.

In order to prove that he is a victim of discrimination, Complainant had to provide evidence to prove that Mr. Burkhardt did not believe the evidence that was presented to him which led him to determine that Complainant was untrustworthy and therefore a threat to national security. Complainant argues that security clearance procedures were not applied fairly to him, but his argument fails because he failed to identify a comparator under applicable EEOC precedent. Specifically, no other employee in the same work unit under the same management officials had their security access suspended for engaging in the same or similar kind of behavior as Complainant, *e.g.*, wearing a wire in the TEC Building and no other employee ever admitted to recording or attempting to record his supervisors on a prior occasion in the TEC Building. Complainant has failed to provide any evidence showing any irregularity in the procedures used to suspend his security access. Accordingly, Complainant has failed to provide evidence that would indicate that the Agency's actions in suspending his security access were motivated by discriminatory animus.

Responsible management officials reasonably believed that Complainant wore a hidden recording device in a secure facility on multiple occasions.

The ERDC-VA-SOP, Physical Security, in place at the relevant timeframe of March 2005, establishes the policy that the ERDC Topographic Engineering Center has been designated a restricted area. ROI at 287. The ERDC-VA-SOP, Physical Security, establishes that TEC work areas are subject to inspection for security purposes.⁸ ROI at 307.

Published Department of the Army security regulation AR 25-2 states that "privately owned receiving, transmitting, recording, amplification and processing equipment is prohibited from use within the confines of any area designated or excluded by the commander to be a ... restricted area." ROI at 230, If 6-5(c). At the time of the Complainant's suspension, TEC had a policy and a practice that prohibited cell phones with camera capability in the TEC Building. AE 5, at 3. The policy is dated 13 January 2003, and signed by Robert W. Burkhardt, it stated, "Cell phones equipped with image capturing capability are not authorized within the facility." AE 5 at 3. A Report of the Military Police Criminal Investigation Command (CID) dated March 16, 2005 ("CID Report") confirms that Police found a "cellphone with camera capabilities for both

⁸At the time of Complainant's arrest, there was a sign posted on the perimeter fence around the TEC Building that said, "Restricted Area." HT at 232.

still images and video" on the Complainant inside the TEC building on March 14, 2005. ROI at 84.⁹

The CID Report documents that Fairfax County Police searched the Complainant inside the TEC Building on March 14, 2005, and that Fairfax County Police Officers found in one of Complainant's pants pockets "a micro cassette recorder with a microphone wired from the recorder, through his shirt sleeve, to his wrist." ROI at 84. That same CID Report indicates that the Police also found a "digital voice recorder" in the Complainant's possession. ROI at 84. The CID Report also states that on March 14, 2005, FBI Special Agent ("SA") Hana played the tape from the Complainant's tape recorder, and that after the preamble by Mr. Campbell, the next recording is the voice of the Fairfax County police officers telling Mr. Campbell he was under arrest. ROI at 86. The CID Report states that on March 14, 2005, SA Hana further told the CID Agent that Mr. Campbell "stated he had recorded another conversation he had with his supervisors." ROI at 86. The record reflects that not only did Complainant at the very least, unsuccessfully attempt to record conversations with his supervisors and/or co-workers, he also admitted to attempting to do so. HT at 90-92; ROI FFC Tr. at 36-38, 42-43; HT at 322-323.

At the hearing, Mr. Burkhardt testified credibly that Complainant did not deny that he had worn a hidden recording device in a secure facility. HT at 289. I therefore find that the totality of the evidence supports the Agency's articulation that it reasonably believed that Complainant wore a hidden recording device on multiple occasions. This belief, established and supported by the facts, clearly establishes the Agency's legitimate, non-discriminatory reason for revoking Complainant's security clearance.

Responsible management officials reasonably believed that Complainant knowingly misrepresented his current residence to his supervisor.

The Agency had evidence at the time of Mr. Burkhardt's decision to substantiate the finding that Complainant misrepresented his current legal residence to his supervisor. On February 9, 2005, the Complainant was read on to a TS/SCI Top Secret Sensitive Compartmented Information security clearance. AE 1 at 3-7. By his signature, the Complainant certified that he would report any change in current residence to the Special Security Officer (SSO) TEC as soon as possible, but not later than 7 days after the change. AE 1 at 5.

Complainant's first line supervisor, Mr. Charles Lopez gave the Complainant the TAB Employee Info Sheet to fill out when he became the Complainant's supervisor. FFC at 39, 184. The TAB Employee Info Sheet contains an entry for "Home Address," followed by a colon and a blank space. AE 3 at 1. The Complainant filled it out, but in the item entitled: "Home Address," instead of listing his current residence, he provided the address of a commercial mail facility. *Id.* at 1; FFC at 38-39. A Memorandum For Record (MFR) dated March 14, 2005, signed by Mr.

⁹Published Department of the Army security regulation AR 380-67 states that individuals must familiarize themselves with pertinent security regulations that pertain to their assigned duties. [ROI at 143, Chap. 9-103(a)].

Charles Lopez, states how he came to doubt the trustworthiness of the Complainant. AE 1 at 28. In the MFR, Mr. Lopez documents that, "after claiming to reside in the vicinity of Huntington Drive and Route 1 in Alexandria, I discovered that the address he had provided me, on two occasions, placed his residence in the Kingstowne section of Fairfax County." *Id.* at 28.

Mr. Harwig testified under oath at the Fact Finding Conference that he asked the Complainant for his current legal address, and that the Complainant never provided it to him. FFC at 127. Nothing in the record proves that the Complainant provided his legal residence to the Agency prior to the decision to suspend him indefinitely. Accordingly, Complainant has failed to meet his burden to prove by a preponderance of the evidence that the Agency acted with discriminatory animus.

Responsible management officials reasonably believed that Complainant created a disturbance in the workplace involving coworkers.

The record contains documentation and testimony that supports Mr. Burkhardt's belief and determination that Complainant created a disturbance in the workplace. Complainant admitted that Mr. Harwig observed him in the Sensitive Compartmented Information Facility, specifically, the workspace of Ms. Kennan and Ms. Hubbard, after he had been transferred out of their workgroup. HT at 71-72. Thus Complainant corroborated Mr. Harwig's Memorandum For Record (MFR) dated February 28, 2005, stating that Mr. Harwig had observed the Complainant on February 25th in the 1000 area of the Sensitive Compartmented Information Facility (SCIF), which is the Source Acquisition Team (SAT) Room. AE 1, at 9; CE 33 at 48.

At the time of the decision in May 2005, Mr. Burkhardt had access to the following evidence which supported his determination that Complainant created a disturbance:

Mr. Harwig's MFR dated February 28, 2005, also states that Ms. Kennan "made reference to instances that sounded to me like stalking: He [Complainant] had looked up her ex-husband on the internet and gotten information on him; He [Complainant] also admitted to Ms. Kerman that he had driven through her neighborhood looking for her house." AE 1 at 9. The MFR states that "Both Alana and Tish revealed many instances where his behavior had made them uncomfortable." *Id.* at 9. The MFR indicates that Mr. Harwig sought advice from TEC Security Office, and in response to their advice, Mr. Harwig removed the Complainant's access to the 1000 area where Ms. Kerman and Ms. Hubbard worked. *Id.* at 9.

The MFR states that Mr Harwig asked Mr. Jeff Popp, Team Leader for the Complainant's team, to talk with the Complainant and document it. AE 1 at 9. The MFR states that Mr. Harwig asked Mr. Popp to inform the Complainant of three things: 1. That his badge access to the 1000 was removed and that he was not to go into that area; 2. That he was not to distract Ms. Kennan or Ms. Hubbard; and 3. That he should minimize his contact with Ms. Hubbard and Ms. Kennan.

Id. On February 28, 2005, Mr. Popp carried out Mr. Harwig's instructions and sent an e-mail to the Complainant and his chain of command. *Id.* at 10.

On March 7, 2005, the Complainant sent an e-mail to his TEC chain of command, the TEC Legal Office, and TEC Security, entitled, "Whistleblowing on aberrant staff behavior," in which he proceeded to make allegations against co-workers Alana Hubbard and Tish Kennan that they were mentally unstable and unprofessional. AE 1 at 11-17. One of his allegations was that Tish Kennan was suffering from "malignant uterine cancer and a hysterectomy" and "being a single parent and having to commute every day across the Wilson Bridge." *Id.* at 16. Complainant alleged that these things made Ms. Hubbard and Ms. Kennan potential security risks. *Id.* at 11-17. Ms. Theresa Rasmussen, the SAT Team Leader, indicated in her testimony about Complainant's email of March 7, 2005, that the contents were of such a personal nature that it caused her to realize that what she had heard about his instability and/or vindictiveness might in fact be true. HT at 410-411.

Mr. Burkhardt indicated in his decision to indefinitely suspend Complainant's security clearance that Complainant did not deny or dispute the reasons stated in the Notice of Proposed Suspension during his oral reply. ROI at 70. Mr. Burkhardt also testified credibly at the hearing that Complainant gave no mitigating circumstances at that same oral reply. HT. at 289. It was therefore reasonable for Mr. Burkhardt to rely on the information above to determine that Complainant had created a disturbance in the workplace involving his co-workers and use it as a contributing factor in his decision to revoke his security clearance.

I therefore find that the aforementioned evidence supports the Agency's articulation that it reasonably believed that Complainant created a disturbance in the workplace with his behaviors. This belief clearly establishes another of the Agency's legitimate, non-discriminatory reason(s) for deciding to revoke Complainant's security clearance.

Responsible management officials reasonably believed that Complainant discussed explosives with his coworkers.

The record reflects that Complainant admitted both at the hearing and during the March 11, 2005, meeting with Burkhardt and Agency management that he had not only discussed his knowledge of explosives with coworkers during off site gatherings, but in fact had also made them. CE 7; HT at 62-64, 94. Once again, the record shows that Complainant offered no mitigating circumstances for his conduct at his opportunity to reply to Mr. Burkhardt's Notice of Proposed Suspension. ROI at 70; HT at 289. Accordingly, the record supports the reasonableness of Mr. Burkhardt's determination.

The gravamen of Complainant's arguments regarding evidence of discrimination, from this Judge's perspective, focused on two or perhaps three areas of the Agency's actions. The first relates to what Complainant apparently perceives as the Agency's disparate treatment of him in comparison to Ms. Hubbard and Ms. Kennan during the period prior to the suspension of his

security clearance. The second relates to the Agency's decision to place him on indefinite suspension without pay pending adjudication of his security clearance. The third area of potential discriminatory Agency action(s) was its decision not to assign Complainant unclassified duties to perform during the adjudication of his security clearance. *See* Complainant's Closing Brief (Complainant's Brief). At the heart of Complainant's arguments regarding these issues is his contention that Ms. Hubbard and Ms. Kennan's contentions regarding his behavior toward him were false and essentially that management knew or should have known the contentions were false. *Id.* at 1-3. I find that the record does not support Complainant's arguments.

Agency's Disparate Treatment of Complainant re Hubbard and Kennan.

Complainant's basic contention is that Ms. Hubbard and Ms. Kennan either were treated differently than he was regarding comments made outside of the office and/or that those alleged comments were not investigated in the same manner as his were. Complainant's Brief at 2-3. Complainant argues that security clearance procedures were not applied fairly to him, but his argument fails because he failed to identify them as valid comparators under applicable EEOC precedent. By the accepted legal standard, these two younger female coworkers, Kennan and Hubbard are not valid comparators for purposes of reviewing security investigations in that they neither made comments regarding making explosives nor wore a hidden recording device in a secured area in the workplace. Additionally, the record reflects that Agency officials did in fact investigate Complainant's allegations regarding Hubbard and Kennan in a similar manner to the way the allegations against him were investigated, *i.e.*, consulting with their managers and coworkers, and found no evidence of wrong doing or inappropriate behavior at that time.

On March 7, 2005, the Complainant sent an e-mail to his TEC chain of command, the TEC Legal Office, and TEC Security, entitled, "Whistleblowing on aberrant staff behavior," in which he proceeded made allegations against co-workers Alana Hubbard and Tish Kerman that they were mentally unstable and unprofessional. AE 1 at 11-17. One of his allegations was that Tish Kerman was suffering from cancer and a hysterectomy. *Id.* at 16. Complainant alleged that these things made Ms. Hubbard and Ms. Kerman potential security risks. *Id.* at 11-17.

On March 8th and 9th, 2005, Paul Harwig investigated the matters raised by the Complainant in his e-mail of March 7, 2005. AE 1 at 20. He individually interviewed Alana Hubbard and Tish Kennan. He asked each if they were under any stress themselves. *Id.* He also interviewed Mary Pat Santoro (Branch Chief); Theresa Rasmussen (Team Leader), and Marty Downing (co-worker), asking whether the person interviewed had any reason to suspect that Mrs. Hubbard or Ms. Kerman showed any behavior, signs of stress, or personal situations that would indicate that they might be a security risk. *Id.* In each interview, the person was in disbelief that Mr. Harwig, would question the emotional stability or reliability of the two women. *Id.* On March 10, 2005, Mr. Harwig reported the results of his investigation to the ERDC Security Office in accordance with AR 380-67 chapter 9-103(b)(5). *Id.*

Based on the totality of the record before me I find that the record fails to support Complainant's contention that he was treated differently than Hubbard and Kennan so as to support an inference of discriminatory disparate treatment. I also find that, at the time, Burkhardt had a reasonable, good faith basis for believing Complainant's managers and coworkers and therefore in making his decision that their testimony did not support Complainant's allegations against Hubbard and Kennan.

Agency's decision to place Complainant on indefinite suspension without pay pending adjudication of his security clearance revocation.

A significant section of Complainant's Brief focused on his contention that he was the victim of disparate treatment when the Agency suspended him without pay pending adjudication of his security clearance revocation. Complainant focused on the 19 employees who had their security clearances suspended but were assigned unclassified duties pending final adjudication of their clearances. Complainant further focused on language that these employees had not committed an overt act (bringing recording equipment onto a secure facility); were not untrustworthy; and/or their character and loyalty were held in high esteem while Complainant's was not. Complainant's Brief at 30-37.

While I agree that these issues could be relevant to this case, I believe the appropriate standard under EEO law, as indicated in the previous section, is that the comparators must have engaged in the same conduct under the same management officials. *Kuracina v. U.S. Postal Service*, Appeal No. 01984991, 2001 EEOPUB LEXIS 6998, (Sep. 20, 2001). A review of the hearings record indicates that none of the 19 employees in question brought recording equipment onto a secure facility, nor did they attempt or admit to attempting to make recordings while within a secure facility - both of which Complainant in fact did. Complainant's Brief at 30-37; Agency Brief at 2-8; HT at 295-311. Specifically, no other employee in the work unit under the same management officials had their security access suspended for wearing a wire in the TEC Building and no other employee ever admitted to recording (or attempting to record) his supervisors on a prior occasion in the TEC Building.

In making his decision, Mr. Burkhardt had access to a document provided by the Security Office which covered the history of all 19 ERDC employees that had lost their security access. ROI at 71; AE 12. Under applicable EEOC precedent, none of those 19 employees are comparators. Only one employee on the list (number 3) had the same management officials as the responsible decision makers in this case. *Id.*; Agency Brief at 6. Employee No. 3, (female, age 49) had the identical security clearance status of TS/SCI as Complainant, but the reasons surrounding the revocation and suspension were not similar in that this employee's clearance was suspended for questionable judgment and reliability due to personal behavior. Her supervisor gave her a written reprimand and arranged for her to meet with an EAP counselor, however, she did not keep the appointment. She was also ultimately terminated by management, unlike Complainant. AE 12 at 2; CE 26 at 2. There were four other employees on the list who had clearance status of TS/SCI, which is the same as Complainant's, specifically, individuals 13; 14;

16; and 17, but all of the security incidents for those employees occurred before Mt. Burkhardt became the Director on October 9, 2001. ROI, FFC at 83, AE 12.

Burkhardt credibly testified extensively and in detail, that based on his review of the record, he made the determination that, unlike Complainant, none of the ERDC employees took any overt action that could have compromised classified information. HT at 295-311. Burkhardt testified at the hearing about the difference between Complainant and the others indicating none of the comparator employees had issues regarding classified material potentially leaving the facility and that both managers and coworkers provided supportive input regarding these employees as to their trustworthiness. *Id.* He indicated, however, that there was no supportive input from management and/or coworkers regarding Complainant's behavior and/or trustworthiness. *Id.*

I therefore find that Complainant has failed to meet the applicable burden of proof, *e.g.*, that of proving, by a preponderance of the evidence, that the legitimate reason proffered by the Agency for suspending his security clearance indefinitely (bringing recording equipment onto a secure facility for the purpose of making clandestine recordings) was a pretext for discrimination.

Agency's decision not to assign Complainant unclassified duties to perform during the adjudication of his security clearance.

Finally, Complainant alleges that the Agency's failure to assign Complainant unclassified duties to perform during the adjudication of his security clearance is indicative of discriminatory animus on its part. The totality of the record fails to support Complainant in this regard. The record reflects that the Agency in fact did explore the possibility of retaining Complainant by assigning him to an interim position with unclassified duties within the Agency, but found that no such position(s) were then available.

The record reflects that the Agency determined there were no vacant positions at ERDC TEC or the other ERDC Office in Alexandria that did not require a secret clearance. At the hearing, Human Resources Specialist Mr. James Klein testified that he conducted a search both locally with the appropriate on site personnel, as well as contacting his peers in the Vicksburg, Hanover and Champaign, Illinois sites. HT at 432-435. On May 19, 2005, Klein sent an e-mail to Ms. Patsy Abbott of the ERDC Deputy Director's Office in which he requested assistance in placing the Complainant in a position located in Alexandria at the Deputy's Office which would not require a security clearance. AE 10. Mr. Klein informed the TEC Deputy Director Mr. Greczy that there were no vacant positions available at the TEC location that did not require at least a secret security clearance. AE 11.

On May 20, 2005, Mr. Harwig made an inquiry of Ms. Santoro, Ms. Rasmussen, and Mr. Downing and determined that Complainant's duties on the SAT required access to classified rooms 50-80 percent of the time. [AE No. 8] That information was provided to Mr. Burkhardt and he considered it in the decision to suspend the Complainant. ROI at 70. Burkhardt therefore

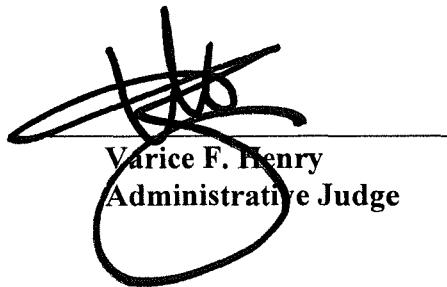
determined that there were no positions available for the Complainant to be reassigned to at ERDC in Alexandria, Virginia. HT at 293.¹⁰

I therefore find that Complainant has failed to meet his burden of proving that the legitimate reason proffered by the Agency for suspending his security clearance indefinitely and not providing him with an interim position working with classified materials was a pretext for discrimination.

CONCLUSION

The record and the hearing testimony support the conclusion that the Agency has articulated legitimate, non-discriminatory reasons for its action. Complainant has failed to rebut the Agency's articulated reasons and failed to provide evidence that he is a victim of discrimination based on his sex, age and/or reprisal. Complainant has not provided evidence from which a fact finder could reasonably conclude that he was a victim of intentional discrimination. The record as a whole supports the Agency's articulated facts. Complainant has not provided evidence sufficient to show that management did not subjectively believe the following: Complainant wore a hidden recording device in a secure facility on multiple occasions; he covertly recorded (or attempted to record) conversation(s) with his supervisor; he failed to give his current legal residence; he created a disturbance in the workplace whereby he boasted to coworkers that he was a person who knew how to make bombs and was charged with stalking a coworker. Ultimately, Complainant simply failed to persuade this Judge that the Agency's actions amounted to intentional discrimination.

For the reasons set forth above, I find that the Complainant did not prove by preponderant evidence that he was discriminated against. Accordingly, I enter judgment in favor of the Agency.



Varice F. Henry
Administrative Judge

¹⁰Contemporaneous documents also support the Agency's legitimate non-discriminatory articulations regarding this issue. On May 25, 2005, Colonel Rowan sent an e-mail to Mr. Burkhardt stating that he was aware that there were no open positions that the Complainant could work in that did not require a security clearance. AE 6 at 1-2.

NOTICE

This is a decision by an Equal Employment Opportunity Commission Administrative Judge issued pursuant to 29 C.F.R. § 1614.109(b), 109(g) or 109(l). **With the exception detailed below, the complainant may not appeal to the Commission directly from this decision.** EEOC regulations require the Agency to take final action on the complaint by issuing a final order notifying the complainant whether or not the Agency will fully implement this decision within forty (40) calendar days of receipt of the hearing file and this decision. The complainant may appeal to the Commission within thirty (30) calendar days of receipt of the Agency's final order. The complainant may file an appeal whether the Agency decides to fully implement this decision or not.

The Agency's final order shall also contain notice of the complainant's right to appeal to the Commission, the right to file a civil action in federal district court, the name of the proper defendant in any such lawsuit and the applicable time limits for such appeal or lawsuit. If the final order does not fully implement this decision, the Agency must also simultaneously file an appeal to the Commission in accordance with 29 C.F.R. § 1614.403, and append a copy of the appeal to the final order. A copy of EEOC Form 573 must be attached. A copy of the final order shall also be provided by the Agency to the Administrative Judge.

If the Agency has *not* issued its final order within forty (40) calendar days of its receipt of the hearing file and this decision, the complainant may file an appeal to the Commission directly from this decision. In this event, a copy of the Administrative Judge's decision should be attached to the appeal. The complainant should furnish a copy of the appeal to the Agency at the same time it is filed with the Commission, and should certify to the Commission the date and method by which such service was made on the Agency.

All appeals to the Commission must be filed by mail, personal delivery or facsimile to the following address:

Director
Office of Federal Operations
Equal Employment Opportunity Commission
131 M Street, NE, 5th Flr.
Washington, D.C. 20507
Facsimile (202) 663-7022

Facsimile transmissions over 10 pages will not be accepted.

COMPLIANCE WITH AN AGENCY FINAL ACTION

An Agency's final action that has not been the subject of an appeal to the Commission or civil action is binding on the Agency. *See* 29 C.F.R. § 1614.504. If the complainant believes that the Agency has failed to comply with the terms of its final action, the complainant shall notify the Agency's EEO Director, in writing, of the alleged noncompliance within thirty (30) calendar days of when the complainant knew or should have known of the alleged noncompliance. The Agency shall resolve the matter and respond to the complainant in writing. If the complainant is not satisfied with the Agency's attempt to resolve the matter, the complainant may appeal to the Commission for a determination of whether the Agency has complied with the terms of its final action. The complainant may file such an appeal within thirty (30) calendar days of receipt of the Agency's determination or, in the event that the Agency fails to respond, at least thirty-five (35) calendar days after complainant has served the Agency with the allegations of noncompliance. A copy of the appeal must be served on the Agency, and the Agency may submit a response to the Commission within thirty (30) calendar days of receiving the notice of appeal.

To:

Walton B. Campbell
6036 Richmond Highway
#211
Alexandria, VA 22303

June D.W. Kalijarvi, Esq.
Kalijarvi, Chuzy & Newman, PC
1901 L Street, NW, Ste. 610
WDC 20036

Timothy Felker, Esq.
Servicing Labor Counsel
U.S. Army Engineer Research & Development Center
CEERD-OC-A, Bldg. 2592
7701 Telegraph Road
Alexandria, VA 22315-3864

Linda S. Wilkinson, EEO Mgr.
ERDC-Army Corps of Engineers
Waterway Experiment Station
3909 Halls Ferry Road
Vicksburg, MS 39180-6199

**U.S. EQUAL EMPLOYMENT OPPORTUNITY COMMISSION
WASHINGTON, D.C. FIELD OFFICE
131 M Street, NE, Suite 0N4W
Washington, D.C. 20507**

Walton B. Campbell, Complainant,) EEOC No. 570-2006-00375X
) Agency No. ARCEERDC08JUL09922
)
v.)
)
Pete Geren, Secretary, Department of the Army, Agency.)
)
)
)
)
	Date: <u>January 13, 2014</u>

ORDER FOR DAMAGES EVIDENCE

Complainant is the prevailing party on the following issue(s):

On August 4, 2005, complainant filed an EEO complaint alleging that he was discriminated against on the bases of sex (male), age (57) and reprisal when on May 27, 2005, he was indefinitely suspended without pay pending a determination of his secret security clearance.

Accordingly, Complainant is ORDERED to provide the undersigned with his/her written claim for damages that were caused by this violation, along with supporting evidence, on or before January 31, 2014.¹ The Agency will have until February 17, 2014, to provide a response to Complainant's request for damages. If either party wishes to have a hearing on the issue of damages, their submission shall so state and provide a basis for this request.

After the submissions have been reviewed, it will be determined if this matter requires a hearing to address damages, at which time a date will be set.

If, after review of the submissions, an additional hearing to address damages is not required, the undersigned will issue a full written decision including the order for damages.

The parties are advised that this matter may be settled until the date the final decision is issued.

¹In light of Complainant's multiple representative(s) and the complexity of the litigation in this case, I am amenable to a request for additional time from the parties to respond to this Order if they find such time is necessary.

ORDER FOR STATEMENT OF ATTORNEY'S FEES

The Complainant in this matter is a prevailing party and therefore may be entitled to an award of attorney's fees and costs. Attorney's fees are only available in actions brought pursuant to Title VII of the Civil Rights Act of 1964, as amended, and the Rehabilitation act of 1973, as amended. 29 C.F.R. § 1614.501(e).

The Complainant is ordered to submit a verified statement of fees and costs accompanied by an affidavit executed by the attorney of record. The method by which attorney fees are calculated is known as the "lodestar," in which the number of hours reasonably expended are multiplied by a reasonable hourly rate.

The statement of attorney's fees and costs must be accompanied by an affidavit executed by the attorney of record itemizing the attorney's charges for legal services. A verified statement of fees and costs shall include the following:

1. A list of services rendered itemized by date, number of hours, detailed summary of the task, rate, and attorney's name;
2. Documentary evidence of reasonableness of hours, such as contemporaneous time records, billing records, or a reasonably accurate substantial reconstruction of time records;
3. Documentary evidence of reasonableness of rate, such as an affidavit stating that the requested rate is the attorney's normal billing rate, a detailed affidavit of another attorney in the community familiar with prevailing community rates for attorneys of comparable experience and expertise, a resume, a list of cases handled, or a list of comparable cases where a similar rate was accepted; and
4. Documentation of costs including, but not limited to, such documentation as receipts, bills, invoices, telephone bills, certified/express mail receipt numbers, per page photo copying rate, and the number of pages photocopied.

The statement of Attorney's fees and costs shall be filed by January 31, 2014. The Agency may respond to the statement of attorney's fees and costs by February 17, 2014. If the Agency disputes the Complainant's verified statement of attorney's fees and/or costs, then the Agency shall file detailed documentation, as previously noted above, in support of its contentions.

Any verified statement of attorney's fees and/or costs and any response filed by the Agency thereto shall comply with the governing regulations, including, but not limited to the pertinent regulations set forth at 29 C.F.R. § 1614.501 (e). The parties should also consult Chapter 11 of EEOC Management Directive.

Failure to comply with any of the Orders in this case or failure to attend any scheduled event may lead to sanctions including the possible dismissal of the captioned complaint(s). *See* 29 C.F.R. §§ 1614.107(a)(7); 109(b); 109(0)(3).

It is so ORDERED.

Varice Ted Henry

Varice Ted Henry
Administrative Judge
Telephone: (202) 419-0717
Facsimile: (202) 419-0740

cc:

June D.W. Kalijarvi, Esq.
Kalijarvi, Chuzy & Newman, PC
1901 L Street, NW, Ste. 610
WDC 20036

202-331-9260
866-452-5789 FAX

jkalijarvi@kcnlaw.com

Timothy Felker, Esq.
Servicing Labor Counsel
U.S. Army Engineer Research & Development Center
CEERD-OC-A, Bldg. 2592
7701 Telegraph Road
Alexandria, VA 22315-3864

703-428-8124
703-428-8154

timothy.l.felker@usace.army.mil



U.S. EQUAL EMPLOYMENT OPPORTUNITY COMMISSION

Office of Federal Operations

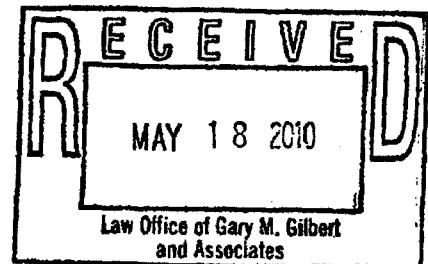
P.O. Box 77960

Washington, DC 20013

Walton B. Campbell,
Complainant,

v.

John M. McHugh,
Secretary,
Department of the Army,
Agency.



Appeal No. 0120080478

Hearing No. 570-2006-00375X

Agency No. ARCEERDC05JUL09922

DECISION

On October 31, 2007, complainant filed an appeal from the agency's October 4, 2007 final order concerning his equal employment opportunity (EEO) complaint alleging employment discrimination in violation of Title VII of the Civil Rights Act of 1964 (Title VII), as amended, 42 U.S.C. § 2000e *et seq.*, and the Age Discrimination in Employment Act of 1967 (ADEA), as amended, 29 U.S.C. § 621 *et seq.* The appeal is deemed timely and is accepted for *de novo* review, pursuant to 29 C.F.R. § 1614.405(a). For the following reasons, the Commission REVERSES the agency's final order.

ISSUE PRESENTED

Whether the EEOC Administrative Judge (AJ) erred in finding that there were no genuine issues of material fact and/or credibility which required resolution at a hearing.

BACKGROUND

At the time of events giving rise to this complaint, complainant worked as a Physical Scientist at the Army Corps of Engineers, Engineer Research and Development Center (ERDC), Topographic Engineering Center (TEC) in Alexandria, Virginia. On August 4, 2005, complainant filed an EEO complaint alleging that he was discriminated against on the bases of

sex (male) and age (57) when, on May 27, 2005, he was indefinitely suspended without pay pending a determination of his secret security clearance.¹

At the conclusion of the investigation, complainant was provided with a copy of the report of investigation and notice of his right to request a hearing before an EEOC Administrative Judge (AJ). Complainant timely requested a hearing. Over complainant's objections, the AJ assigned to the case granted the agency's November 2, 2006 motion for a decision without a hearing ("Motion") and issued a decision without a hearing on September 19, 2007, in favor of the agency.

AJ Decision

At the outset, the AJ agreed with the agency's assertion that complainant failed to establish a *prima facie* case of sex or age-based discrimination. Specifically, the AJ found that complainant did not show that others, not in his protected group, were treated differently under similar circumstances. The AJ noted that complainant identified two younger female co-workers who reported him to management as a potential security risk approximately 10 days after complainant reported them as security risks. The AJ noted that complainant came under scrutiny for wearing a hidden recording device at the workplace, recording his supervisors, failing to provide management with his home address (legal residence), and creating a "disturbance" in the workplace. The AJ found that complainant provided no evidence showing that either of the alleged comparators engaged in similar activities.

The AJ further found that the agency proffered reasonable and legitimate non-discriminatory reasons for its actions. According to the AJ, the agency produced evidence that it acted properly under national security laws and regulations in suspending complainant's access to classified information and in subsequently suspending him indefinitely without pay.

The AJ then found that complainant did not provide preponderant evidence from which a fact finder could reasonably conclude that he was the victim of intentional discrimination. The AJ found that the record as a whole supported the agency's articulated facts, and complainant did not provide evidence of the state of mind of the responsible managerial officials sufficient to show that they did not subjectively believe that the allegations against complainant could be true (e.g. that complainant wore a hidden recording device in a secure facility on multiple occasions; that he failed to give his current legal residence; and that he created a disturbance in the workplace). The AJ then found no discrimination. The agency subsequently issued a final order adopting the AJ's finding that complainant failed to prove that he was subjected to discrimination as alleged.

¹ Neither the decision to review his security clearance nor the outcome of the review is at issue here. Complainant's claim is that the agency discriminated against him by not allowing him to continue working while his security clearance was under review.

CONTENTIONS ON APPEAL

On appeal, complainant, through counsel, contends that there are genuine issues of fact in dispute regarding the agency's reasons for suspending him which are clearly material to whether or not the suspension was discriminatory. Specifically, complainant notes the following: on March 14, 2005, he was formally debriefed about his Top Secret/SCI clearances and his access to classified information was withdrawn. Management proposed his indefinite suspension on April 27, 2005, and the agency issued a decision letter suspending him on May 27, 2005. Complainant, however, points out that between March 14 and May 27, he was performing work even though he no longer had a security clearance. Complainant's supervisor reported that "[complainant's] current duties did not require for him to have access to classified information." Complainant's Team Leader testified that during this period, "[complainant] was doing the things I gave him to do and he was getting them done on time." On March 21, 2005, complainant's Supervisor notified Security that, "There is no restriction on his [complainant's] use of the unclassified network." Complainant contends that, as of March 21, 2005, his management was fully aware that he was performing his assigned tasks without access to any classified materials. Complainant contends that this evidence clearly disputes, and if found credible, rebuts the agency's articulated reasons for suspending complainant without pay.

Complainant also contends that the agency treated him less favorably than his two younger female co-workers (C1 and C2). Specifically, complainant contends that the agency treated C1 and C2 differently with regard to how they reacted and investigated the allegations of untrustworthiness and security violations by them and by complainant respectively and, as such, is liable for the resultant damages.² Complainant contends that the agency is not relieved from liability merely because C1 and C2's access to classified information and security clearances was not removed.

In response to the appeal, the agency contends that the AJ properly found that complainant did not establish a *prima facie* case of discrimination or provide evidence that the agency's reasons were pretextual. The agency also asserts that the AJ properly found that there were no genuine issues of material fact in dispute or that any credibility determinations were required. In addition, the agency asserts that, based on the uncontradicted evidence in the record, there is no support for complainant's argument that a finder of fact could conclude that his "security clearance suspension" did not require suspending his employment. Therefore, the agency asks the Commission to affirm its final order.

² Complainant alleged that one of the younger females stated to him in normal conversations that she was an ex-Marine, was a good marksman and knew how to shoot. Complainant indicated that he feared her because of these statements. ROI, Ex. F-8.

ANALYSIS AND FINDINGS

At the outset, we note that, as this is an appeal from a FAD issued without a hearing, pursuant to 29 C.F.R. § 1614.110(b), the agency's decision is subject to *de novo* review by the Commission. 29 C.F.R. § 1614.405(a). The Commission's regulations allow an AJ to issue a decision without a hearing when he or she finds that there is no genuine issue of material fact. 29 C.F.R. § 1614.109(g). This regulation is patterned after the summary judgment procedure set forth in Rule 56 of the Federal Rules of Civil Procedure. The U.S. Supreme Court has held that summary judgment is appropriate where a court determines that, given the substantive legal and evidentiary standards that apply to the case, there exists no genuine issue of material fact. *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 255 (1986). In ruling on a motion for summary judgment, a court's function is not to weigh the evidence but rather to determine whether there are genuine issues for trial. *Id.* at 249. The evidence of the non-moving party must be believed at the summary judgment stage and all justifiable inferences must be drawn in the non-moving party's favor. *Id.* at 255. An issue of fact is "genuine" if the evidence is such that a reasonable fact finder could find in favor of the non-moving party. *Celotex v. Catrett*, 477 U.S. 317, 322-23 (1986); *Oliver v. Digital Equip. Corp.*, 846 F.2d 103, 105 (1st Cir. 1988). A fact is "material" if it has the potential to affect the outcome of the case. If a case can only be resolved by weighing conflicting evidence, issuing a decision without holding a hearing is not appropriate. In the context of an administrative proceeding, an AJ may properly consider issuing a decision without holding a hearing only upon a determination that the record has been adequately developed for summary disposition. See *Petty v. Department of Defense*, EEOC Appeal No. 01A24206 (July 11, 2003).

The courts have been clear that summary judgment is not to be used as a "trial by affidavit." *Redmand v. Warrener*, 516 F.2d 766, 768 (1st Cir. 1975). The Commission has noted that when a party submits an affidavit and credibility is at issue, "there is a need for strident cross-examination and summary judgment on such evidence is improper." *Pedersen v. Department of Justice*, EEOC Request No. 05940339 (February 24, 1995). "Truncation of this process, while material facts are still in dispute and the credibility of witnesses is still ripe for challenge, improperly deprives complainant of a full and fair investigation of her claims." *Mi S. Bang v. United States Postal Service*, EEOC Appeal No. 01961575 (March 26, 1998); see also *Peavley v. United States Postal Service*, EEOC Request No. 05950628 (October 31, 1996); *Chronister v. United States Postal Service*, EEOC Request No. 05940578 (April 23, 1995). The hearing process is intended to be an extension of the investigative process, designed to "ensure that the parties have a fair and reasonable opportunity to explain and supplement the record and to examine and cross-examine witnesses." See EEOC Management Directive (MD) 110, November 9, 1999, Chapter 6, page 6-1; see also 29 C.F.R. § 1614.109(d) and (e).

Next, we note that the Commission has issued decisions affirming the dismissal of complaints contesting the decision to revoke or deny a security clearance, finding that such claims fail to state a claim pursuant to 29 C.F.R. § 1614.107(a)(1). See, e.g., *Rezaee v. Department of the*

Air Force, EEOC Appeal No. 01A60451 (April 25, 2006); *Carr v. Department of the Army*, EEOC Appeal No. 01A44011 (November 4, 2004). However, the Commission has reviewed whether the grant, denial, or revocation of a security clearance was carried out in a discriminatory manner. *Id.*; *Dodson v. Department of Defense*, EEOC Appeal No. 01954101 (June 13, 1997) (the Commission found discrimination where a manager sought to have an employee's clearance revoked in retaliation for filing EEO complaints); *Schroeder v. Department of Defense (Defense Mapping Agency)*, EEOC Request No. 05930248 (April 14, 1994). As previously noted, the instant case concerns complainant's challenge to the decision to suspend him indefinitely without pay, instead of continuing to provide him with work that was not classified, while awaiting a determination on his security clearance. The issue clearly states a viable claim that can be properly adjudicated within the EEO complaints process.

Complainant claims there were unclassified duties he could have performed, and that he had in fact been permitted to do them for a period of time, but management chose not to allow that anymore because of discrimination. The agency denies that such work was available for complainant, and/or even if it were available, denies that it had the obligation to provide complainant with such work, noting that "[u]nder the circumstances, [complainant's] retention in duty status would be detrimental to national security interests." May 27, 2005 Decision Notice. We note, however, the testimony of complainant's Supervisor and Team Leader that complainant's current duties did not require him to have access to classified information; he was doing the things he was given and performing his duties in a timely manner; and that there were no restrictions on his use of the unclassified network.

Because, at the summary judgment stage, complainant's evidence must be believed and all justifiable inferences drawn in his favor, we find that judgment as a matter of law should not have been granted in this case as the record contains genuine issues for trial. There is clearly a genuine material issue of fact in dispute concerning why management decided that complainant needed to be suspended without pay after he had been allowed to continue working between March 14, 2005 (when he was formally debriefed and his clearances and access to classified information was withdrawn), and May 27, 2005 (when the agency issued a decision letter suspending him).

Complainant asserts that the decision to place him on suspension without pay was discretionary, as the agency did not have a policy that an individual must be suspended if his or her security clearance was suspended. Complainant contends that in fact, the opposite was true - no employee had ever been indefinitely suspended without pay due to a suspended or revoked security clearance. The agency's response to this is that no prior employee had ever been found to have committed any "overt act," as complainant was found to have done (*i.e.*, by bringing recording equipment onto secured property). In any event, there is clearly a need for a credibility determination as to whether complainant's case was in fact, as different as management claims, from the cases of others whose security clearance came under review in the past.

Finally, we note that the May 27, 2005 Decision letter indicates that a reason complainant was being suspended was that he "created a disturbance in the workplace involving coworkers. Specifically, you boasted to co-workers that you were a person who sought revenge and knew how to make bombs." Complainant denies that he ever made such statements and asserts that none of his coworkers testified that they ever heard him threaten or attempt to take revenge on anybody or threaten or attempt to blow anybody up with any bombs. He also notes that his Supervisor "is not credible because his official documentary accounts and sworn testimony regarding what he was told by [the younger female co-workers] during their single meeting on February 25, 2005, has materially and repeatedly changed. He also questions why he would have been permitted to continue working at all if he had truly made bomb-related threats or comments.

The hearing process is intended to be an extension of the investigative process, and is designed to ensure that the parties have "a fair and reasonable opportunity to explain and supplement the record and, in appropriate instances, to examine and cross-examine witnesses." *See* Equal Employment Opportunity Management Directive for 29 C.F.R. Part 1614 (EEO MD-110), 7-1 (November 9, 1999); *see also* 29 C.F.R. § 1614.109(e). "Truncation of this process, while material facts are still in dispute and the credibility of witnesses is still ripe for challenge, improperly deprives complainant of a full and fair investigation of her claims." *Mi S. Bang v. United States Postal Service*, EEOC Appeal No. 01961575 (March 26, 1998). *See also* *Peavley v. United States Postal Service*, EEOC Request No. 05950628 (October 31, 1996); *Chronister v. United States Postal Service*, EEOC Request No. 05940578 (April 25, 1995). In summary, there are simply too many unresolved issues which require an assessment of the credibility of the parties, and the reason for complainant's suspension.

CONCLUSION

In this case, issuance of a decision without a hearing was not warranted under 29 C.F.R. § 1614.109(g). The Commission REVERSES the agency's final order and REMANDS the matter for a hearing in accordance with this decision and the ORDER below.

ORDER

The agency shall submit to the Hearings Unit of the Washington Field Office the request for a hearing within fifteen (15) calendar days of the date this decision becomes final. The agency is directed to submit a copy of the complaint file to the EEOC Hearings Unit within fifteen (15) calendar days of the date this decision becomes final. The agency shall provide written notification to the Compliance Officer at the address set forth below that the complaint file has been transmitted to the Hearings Unit. Thereafter, the Administrative Judge shall issue a decision on the complaint in accordance with 29 C.F.R. § 1614.109 and the agency shall issue a final action in accordance with 29 C.F.R. § 1614.110.

IMPLEMENTATION OF THE COMMISSION'S DECISION (K0501)

Compliance with the Commission's corrective action is mandatory. The agency shall submit its compliance report within thirty (30) calendar days of the completion of all ordered corrective action. The report shall be submitted to the Compliance Officer, Office of Federal Operations, Equal Employment Opportunity Commission, P.O. Box 19848, Washington, D.C. 20036. The agency's report must contain supporting documentation, and the agency must send a copy of all submissions to the complainant. If the agency does not comply with the Commission's order, the complainant may petition the Commission for enforcement of the order. 29 C.F.R. § 1614.503(a). The complainant also has the right to file a civil action to enforce compliance with the Commission's order prior to or following an administrative petition for enforcement. See 29 C.F.R. §§ 1614.407, 1614.408, and 29 C.F.R. § 1614.503(g). Alternatively, the complainant has the right to file a civil action on the underlying complaint in accordance with the paragraph below entitled "Right to File A Civil Action." 29 C.F.R. §§ 1614.407 and 1614.408. A civil action for enforcement or a civil action on the underlying complaint is subject to the deadline stated in 42 U.S.C. 2000e-16(c) (1994 & Supp. IV 1999). If the complainant files a civil action, the administrative processing of the complaint, including any petition for enforcement, will be terminated. See 29 C.F.R. § 1614.409.

STATEMENT OF RIGHTS - ON APPEALRECONSIDERATION (M1208)

The Commission may, in its discretion, reconsider the decision in this case if the complainant or the agency submits a written request containing arguments or evidence which tend to establish that:

1. The appellate decision involved a clearly erroneous interpretation of material fact or law; or
2. The appellate decision will have a substantial impact on the policies, practices, or operations of the agency.

Requests to reconsider, with supporting statement or brief, must be filed with the Office of Federal Operations (OFO) within thirty (30) calendar days of receipt of this decision or within twenty (20) calendar days of receipt of another party's timely request for reconsideration. See 29 C.F.R. § 1614.405; Equal Employment Opportunity Management Directive for 29 C.F.R. Part 1614 (EEO MD-110), 9-18 (November 9, 1999). All requests and arguments must be submitted to the Director, Office of Federal Operations, Equal Employment Opportunity Commission, P.O. Box 77960, Washington, DC 20013. In the absence of a legible postmark, the request to reconsider shall be deemed timely filed if it is received by mail within five days of the expiration of the applicable filing period. See 29

C.F.R. § 1614.604. The request or opposition must also include proof of service on the other party.

Failure to file within the time period will result in dismissal of your request for reconsideration as untimely, unless extenuating circumstances prevented the timely filing of the request. Any supporting documentation must be submitted with your request for reconsideration. The Commission will consider requests for reconsideration filed after the deadline only in very limited circumstances. *See* 29 C.F.R. § 1614.604(c).

COMPLAINANT'S RIGHT TO FILE A CIVIL ACTION (R0408)

This is a decision requiring the agency to continue its administrative processing of your complaint. However, if you wish to file a civil action, you have the right to file such action in an appropriate United States District Court within ninety (90) calendar days from the date that you receive this decision. In the alternative, you may file a civil action after one hundred and eighty (180) calendar days of the date you filed your complaint with the agency, or filed your appeal with the Commission. If you file a civil action, you must name as the defendant in the complaint the person who is the official agency head or department head, identifying that person by his or her full name and official title. Failure to do so may result in the dismissal of your case in court. "Agency" or "department" means the national organization, and not the local office, facility or department in which you work. Filing a civil action will terminate the administrative processing of your complaint.

RIGHT TO REQUEST COUNSEL (Z1008)

If you decide to file a civil action, and if you do not have or cannot afford the services of an attorney, you may request from the Court that the Court appoint an attorney to represent you and that the Court also permit you to file the action without payment of fees, costs, or other security. *See* Title VII of the Civil Rights Act of 1964, as amended, 42 U.S.C. § 2000e *et seq.*; the Rehabilitation Act of 1973, as amended, 29 U.S.C. §§ 791, 794(c). The grant or denial of the request is within the sole discretion of the Court. Filing a request for an

attorney with the Court does not extend your time in which to file a civil action. Both the request and the civil action must be filed within the time limits as stated in the paragraph above ("Right to File A Civil Action").

FOR THE COMMISSION:



Carlton M. Hadden, Director
Office of Federal Operations

MAY 14 2010

Date

CERTIFICATE OF MAILING

For timeliness purposes, the Commission will presume that this decision was received within five (5) calendar days after it was mailed. I certify that this decision was mailed to the following recipients on the date below:

Walton B. Campbell
9901 Stoneybrook Dr
Kensington, MD 20895

Gary M. Gilbert, Esq.
8401 Colesville Rd #315
Silver Spring, MD 20910

Spurgeon A. Moore, Director
EEO Compliance & Complaints Review
Department of the Army
1901 South Bell Street
Crystal Mall 4, Suite 109B
Arlington, VA 22202-4508

MAY 14 2010

Date



Equal Opportunity Assistant

Donte Newman

From: DocuManager Powered by Fax2Mail [reports@reply.fax2mail.com]
Sent: Monday, August 22, 2011 3:14 PM
To: Donte Newman
Subject: Walton Campbell

MAIL2FAX DETAILED DELIVERY REPORT	
Attention	Donte Newman
Job Number	62722150
Sent By User	F2M/93519869174
Entered Fax2Mail System	08/22 15:05
Report Generated	08/22 15:14
Subject	Walton Campbell
Page Count	24 (including cover sheet)

SUMMARY		
Sent: 1	Errors: 0	Cancelled: 0
Total: 1		

Destination	Status	Date	Time	Num. Retries
2025640356	SENT	08/22	15:11	1



DEPARTMENT OF DEFENSE
DEFENSE LEGAL SERVICES AGENCY
DEFENSE OFFICE OF HEARINGS AND APPEALS
WASHINGTON HEARING OFFICE
POST OFFICE BOX 3627
ARLINGTON, VIRGINIA 22203-1995
FAX (703) 696-1831



DATE: SEP 05 2007

In re:)
CAMPBELL, Walton Bayne)
██████████)
Appellant in Personal Appearance)

**Security Clearance
Granted by PSAB**

USA-C No. 07-07329

**RECOMMENDED DECISION OF ADMINISTRATIVE JUDGE
MARK W. HARVEY**

APPEARING FOR APPELLANT
David P. Price, Esquire

SYNOPSIS

Appellant had three alleged security violations, and several other alleged transgressions listed on his statement of reasons. The U.S. Army Central Personnel Security Clearance Facility (USA CCF) informed Appellant that the transgressions alleged under the personal conduct guideline did not constitute a security concern. The evidence did not establish that Appellant violated any security rules or regulations. I recommend that the Department of the Army Personnel Security Appeals Board overturn the letter revoking his eligibility for access to SCI information and his access to classified information.

HISTORY OF CASE

On December 13, 2005, the U.S. Army Central Personnel Security Clearance Facility (USA CCF) issued Appellant a Letter of Intent (LOI) to Revoke Sensitive

FOR OFFICIAL USE ONLY
When unredacted this document contains information
EXEMPT FROM MANDATORY DISCLOSURE under the FOIA
Exemption 6 applies

1

Compartmented Information (SCI) Access Eligibility and Security Clearance.¹ The LOI detailed reasons why the USA CCF could not make a preliminary affirmative finding that it is clearly consistent with the interests of national security to grant or continue Appellant's security clearance and eligibility for SCI access. Specifically, the LOI forwarded a Statement of Reasons (SOR) setting forth security concerns arising from Appellant's personal conduct and security violations.

On March 9, 2006, Appellant responded in writing to the LOI, providing information on the SOR allegations. The USA CCF issued a letter revoking his eligibility for access to SCI information and his access to classified information (LOR) on September 27, 2006. The LOR indicated his personal conduct and the security violations remained a security concern. On October 10, 2006, he requested a personal appearance before an administrative judge from the Defense Office of Hearings and Appeals (DOHA).² On October 13, 2006, Lieutenant Colonel Ralph, Deputy Commander, USA CCF, informed Appellant's counsel that all SOR allegations were mitigated except for the three security violations (pages of documents admitted (pg.) 41-43). Nevertheless, this decision will briefly address all SOR allegations, as some provide background information, explaining Appellant's motive for tape recording a conversation in the workplace.

On June 8, 2007, DOHA received the case, and assigned it to me. Appellant's lawyer requested a delay until July 6, 2007. A notice of personal appearance was issued on June 13, 2007. The personal appearance was held on July 6, 2007. DOHA received the record of the hearing (R.) on July 18, 2007. Appellant provided documentation pertaining to the security concerns, and I admitted 44 pages of documents into the record.

¹ The LOI was issued under Department of Defense (DoD) Directive 5200.2-R, January 1987, *Personnel Security Program*, as amended and modified (Regulation), Army Regulation 380-67, September 9, 1988, Department of the Army Personnel Security Program Regulation, as amended by Memorandum, DAMI-CH, February 19, 1999, Subject: Personnel Security, and Memorandum, IACF-AD, December 13, 2005, Subject: Intent to Revoke Sensitive Compartmented Information (SCI) Access Eligibility and Security Clearance.

² Authority and criteria for the personal appearance arises from Executive Order 12968, *Access to Classified Information*, dated August 4, 1995, as implemented by the Regulation, Department of Defense Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (Directive), dated January 2, 1992, as amended, modified and revised, as well as the references cited in note 1, *supra*.

On August 30, 2006, the Under Secretary of Defense (Intelligence) published a memorandum directing application of revised Adjudicative Guideline to all adjudications and other determinations made under the Directive and the Regulation in which the SOR was issued on or after September 1, 2006. The revised Adjudicative Guidelines (AG) do not apply to this case because the SOR was issued prior to September 1, 2006.

FOR OFFICIAL USE ONLY
When unredacted this document contains information
EXEMPT FROM MANDATORY DISCLOSURE under the FOIA
Exemption 5 applies

FINDINGS OF FACT

Appellant is a 60-year-old civilian employed by Department of the Army as a scientist. He married in 1971, and was divorced in 1981 (Questionnaire for National Security Positions (SF 86)). In 1981, Appellant received a Ph.D from the University of Georgia in Marine Ecosystems (R. 16; SF 86). He did not serve in the military (SF 86). He worked for the Bank of New York on Wall Street for five years (R. 16), and then for the National Oceanic and Atmospheric Administration (NOAA) for 17 years (R. 16). He received the NOAA Administrator's Award for his contributions during Operation Desert Storm (R. 17; File at 257). He also received the Department of Commerce's Gold and Bronze Awards for saving lives and money in 1997 and 1994, respectively (R. 17; File at 44, 238, 256, 257). Next, he worked for the Naval Research Laboratory (NRL) (R. 18). At the NRL, he had some performance difficulties concerning attracting funding for research projects, and he was placed on a performance improvement plan (R. 18; File at 273-274). The NRO sent him to the National Park Service for a two-year detail, and at the conclusion of that assignment, he lost his NRL job due to a reduction in force (R. 19; File at 258). On July 26, 2004, he received a job with Topographic Engineering Center in Alexandria, VA, under the Priority Placement Program (R. 19-20). Appellant has periodically held a security clearance during the last 20 years (File at 44).

SOR ¶ 1.a (security violation)

Between January 1999 and May 2000, while Appellant was employed at the NRL, a security clearance background investigator wanted to interview him in private concerning several of his subordinates (R. 20-21; File at 45). A Sensitive Compartmented Information Facility (SCIF) conference room was next to Appellant's office (R. 22). The SCIF conference room was not used to store classified materials (R. 23). Appellant ensured no classified documents were inadvertently left in the SCIF conference room (R. 22). One employee was in the area, and Appellant told the employee of the confidential interview to ensure no classified information was discussed, and the employee did not hear Appellant discuss private information with the investigator (R. 23). Appellant checked the identification and credentials of the investigator (File at 45). Appellant escorted the investigator throughout the time he was inside Appellant's building (R. 24). Appellant assumed the investigator was as reliable and responsible as someone who fixes the plumbing or cleans the area (R. 24). Subsequently a security officer verbally warned Appellant about allowing an un cleared person into a SKIF. See SOR ¶ 1.a.³ The Office of Personnel Management (OPM) interview indicates Appellant

³ DCI 6/4, *Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information*, July 2, 1998, paragraph 6-105 provides that non-Program-briefed personnel, such as maintenance or repair personnel, visiting a Special Access Program Facility, will sign-in a visitor's record, and be escorted at all times. Sanitization procedures will be implemented in advance. DCI 6/9, *Physical Security Standards for Sensitive Compartmented Information Facilities*, November 18, 2002, paragraph 2.5.2 requires each SCIF to

received a "note of caution" concerning the incident (File at 261). Appellant was never told that he violated any particular regulation, and he complied with the security officer's caution about handling of SKIF visitors (R. 26-27). Uncleared visitors are permitted in a SKIF provided the area is sanitized and the visitor is escorted. *See note 3, supra.* Appellant met both these criteria. Appellant said he was not aware that his conduct violated any security rule (R. 121-122). The record evidence does not allege a particular security rule was violated. **I conclude that the evidence does not establish violation of any security rules.**

SOR ¶ 1.b (damage to a yard cart and retention of a shed key)⁴

Between 1999 and 2003, Appellant borrowed a yard cart from a neighbor, and used the neighbor's tools and tool shed (File at 46, 270). His neighbor has some psychological problems, and her description of her interactions with Appellant are not completely accurate (File at 46). He damaged the bicycle-type wheels on the cart, and did not offer to pay for the damaged cart. *Id.* The neighbor gave the cart to Appellant. *Id.* The owner of the cart did not ask him to pay for the cart. *Id.* LTC Denton provided a statement indicating the rim of the yard cart's wheel was damaged, and Appellant repaired the damage. (File at 68). Appellant gave the cart to LTC Denton, who continued to use the cart until he left Louisiana in December 2005. *Id.* Appellant mistakenly retained the neighbor's shed key after he left Louisiana; however, when he returned to Louisiana for a visit, he returned the key to her.⁵ *Id.* The evidence does not establish that he violated a rule.

SOR ¶¶ 1.c and 1.d (security violation)

SOR ¶¶ 1.c and 1.d allege on December 18, 2000, Appellant gave classified information concerning satellite capabilities to a National Public Radio reporter, who interviewed him during a trip to Antarctica. A security manager at NRL opined that the National Science Foundation (NSF) investigated the allegation (File at 278). The security manager did not provide details about why she believed this to be true. The OPM ROI indicates:

A copy of an internet article dated 12/18/00 by a National Public Radio (NPR) reporter contains statements by the subject about the capabilities

have procedures for identification and control of visitors seeking access to the SCIF. In this case, those procedures were not provided.

⁴ The USA CCF advised Appellant's counsel that this allegation was not a security concern on November 8, 2006 (pg. 41-43). This brief discussion concurs with that USA CCF assessment.

⁵ Appellant's statement (File at 46-47) provides additional details about his relationship with his neighbor, the damaged cart, and the belatedly returned shed key.

of U.S. satellites.⁶ He was interviewed by the reporter while on a research project in Antarctica studying penguin movements by satellite. He told the reporter that he used his military connections and arranged to have two spy satellites take pictures of the penguins. His record contains no information or documentation of an inquiry into the matter. There is no indication of any actions against the subject related to this matter.

File at 272-273. Appellant described the reason the NPR reporter included his name in the article, and provided the location of the NPR article on the internet (File at 50). A NSF public affairs officer was present when Appellant was interviewed (File at 50-51). Appellant insists that he did not provide classified information to the NPR reporter, and the NPR article does not attribute to Appellant any classified information (File at 50-51). There is no record evidence that the information he revealed to NPR was classified. This allegation is not established.

SOR ¶¶ 1.c to 1.e (filing grievances and complaints)⁷

SOR ¶¶ 1.c to 1.e allege Appellant abused the grievance system by making allegations and complaints. Other sources questioned Appellant's honesty and judgment, apparently related to his filing of grievances and complaints against NRL. SOR ¶¶ 1.f and 1.h.⁸ A source indicated Appellant wanted a security clearance, even though it was unnecessary for his NRL job (File at 278). Other witnesses were aware of Appellant's allegations at NRL, and questioned his loyalty to NRL.

An attorney from the legal office more specifically described Appellant's complaints about NRL irregularities, and did not indicate Appellant's allegations were in bad faith or factually false. The attorney represented the government at the Appellant's MSPB proceeding, and as a government advocate his interests were opposed to Appellant's interests. He described Appellant as "a stickler for close attention to all rules and regulations." (File at 49, 275). Appellant's complaints pertained to NRL budget, payroll, and hiring irregularities (File at 275-277). **NRL did not contest the legitimacy of Appellant's complaints and settled the personnel action that was taken against him. *Id.***

The overall OPM investigation and Appellant's materials revealed more witnesses who support Appellant than witnesses who question his motivation for

⁶ The article states, "So Campbell figured he'd use his military connections. He says he's arranged for two spy satellites to take pictures through clouds. He'll be on the ground taking pictures for comparison." File at 196.

⁷ See note 4, *supra*.

⁸ The NRL source(s) for SOR ¶¶ 1.c and 1.d are likely to be biased against Appellant because Appellant made allegations against the sources (File at 273-274).

making complaints and filing grievances at NRL. His allegations were made in good faith, and are based in fact. The record evidence does not establish that he violated a rule.

SOR ¶ 1.g (stalking)⁹

From July 2004 until approximately February 2005, Appellant frequently went to lunch with several employees of the Operations Division, Engineering Research and Development Center (ERDC), including Ms. Kennon and Ms. Hubbard (R. 34-35; 53-54; 58-61; File at 57). In February 2005, Appellant moved into the same division where Ms. Kennon and Ms. Hubbard worked (R. 35). On February 25, 2005, Mr. Harwig a senior employee at ERDC, noticed Appellant "sitting too close" to Ms. Kennon and Ms. Hubbard and looking over their shoulders at a workstation they were using (File at 164). Later that day, Mr. Harwig questioned them about their relationships with Appellant. *Id.* Ms. Kennon said Appellant looked up her ex-husband on the internet, and drove through her neighborhood looking for her house. *Id.* Ms. Hubbard said she felt uncomfortable around Appellant.¹⁰ *Id.*

On February 28, 2005, Appellant was invited to go to the customary lunch with Ms. Kennon and Ms. Hubbard (R. 61-62). Appellant was not informed that Ms. Kennon and Ms. Hubbard did not want to have lunch with him until he was counseled about his relationship with them on February 28, 2005 (R. 133-134; pg. 33-34). Later, on February 28, 2005, Appellant's supervisor sent him an e-mail stating he was distracting the female employees on February 25, 2005. In the e-mail he directed Appellant to stay out of the office areas where Ms. Kennon and Ms. Hubbard worked, and to minimize his contact with them (R. 62-63; File at 165; pg. 16, 19). Appellant was very upset about the email, and considered it an official document alleging improper conduct (R. 64-65).

On March 7, 2005, Appellant sent a lengthy e-mail to eight of his supervisors denying any misconduct and making a variety of allegations against Ms. Kennon and Ms. Hubbard (R. 65-67; pg. 17A-17G; File at 166-172). Some of his allegations raised security concerns, and/or alleged Ms. Kennon and/or Ms. Hubbard displayed organizational disloyalty by making derogatory comments about the Army and their

⁹ See note 4, *supra*.

¹⁰ Appellant used the internet to attempt to locate a co-worker to call about extending his leave while he was in Mexico, and happened to find a link to Ms. Kennon's former husband while surfing the internet (R. 78-81; File at 58). Appellant denied the allegation that he was driving around Ms. Kennon's neighborhood looking for her residence (R. 82). He drove to his old neighborhood (where he lived for 17 years) to visit old neighbors. His former residence was in the same town where Ms. Kennon's residence was located. He mentioned at the lunches that he found her former husband's phone number on the internet, and went to Ms. Kennon's town, adding to her concerns that he was stalking her. Appellant also gave Ms. Kennon inexpensive, unsolicited gifts of ear plugs, a battery cleaner, a book and candy (File at 176).

supervisors at a public restaurant (R. 61-62). On March 8, 2007, Appellant was counseled about sexual harassment¹¹ without being provided any factual description of his alleged harassing behavior (R. 68). Appellant subsequently learned that Ms. Kennon said he often looked at her breasts and told her once she "look[ed] like trouble;" however, Appellant said her description was a misquote (R. 113-116). The reaction of Appellant's supervisors to his lengthy e-mail of March 7, 2005, was negative, as they questioned his judgment and stability (pg. 33-34).

On March 9, 2007, after work, Appellant went to the gym with Laura Mulholland, an ERDC employee (R. 71; File at 59). After working out for about an hour, he drove his normal route home via Telegraph Road, to Huntington, to Route One, and then to his apartment in Alexandria (R. 71-72; File at 59). Ms. Kennon usually drives home via Telegraph Road, to Huntington, and then Route One to the Beltway (R. 74). On March 9, 2007, Ms. Kennon left her office, and on her way home, she noticed Appellant in his vehicle as she drove through an intersection (File at 176). She turned around, and returned to the office to report him for following her (File at 59, 176).

On March 10, 2007, Mr. Harwig told Appellant he was under investigation for misconduct, to avoid contact with Ms. Kennon and Ms. Hubbard, and he suspended Appellant's access to the SKIF (R. 69; pg. 18). On March 11, 2007, Appellant attended a meeting chaired by Mr. Harwig and attended by law enforcement and security representatives, and he was accused of stalking Ms. Kennon by following her home on March 9, 2007 (R. 70-71).

On March 11, 2007, at about 4:00 p.m., Ms. Kennon signed a Fairfax County arrest warrant accusing Appellant of stalking her (R. 73).

Mr. Harwig responded to Appellant's allegations by asking Ms. Kennon and Ms. Hubbard and their supervisors whether Ms. Kennon and/or Ms. Hubbard were under stress or were unreliable (File at 175; pg. 20). Apparently Mr. Harwig did not confront them with Appellant's specific allegations. *Id.* The supervisor determined Appellant's allegations were unfounded, and no further investigation was warranted. *Id.*

On March 11, 2005, Mr. Harwig interviewed Appellant about the allegations. (File at 177-178). Appellant said he went to the gym to work out. *Id.* After working out he drove home. *Id.* His route home is similar to Ms. Kennon's. *Id.* He did not see her, or knowingly follow her (File at 178).

On October 19, 2005, Appellant was found not guilty of stalking (File at 60).

¹¹ The SOR did not allege Appellant committed sexual harassment. Thus, sexual harassment cannot be used as a basis to deny his security clearance.

SOR ¶¶ 1.g and 1.h (security violation)

On March 10, 2005, Appellant brought a tape recording device to his office because he wanted to record Ms. Kennon and/or counseling sessions with his supervisors (R. 84-88; File at 60). He believed Mr. Harwig and Ms. Kennon had a special relationship (R. 85-86). He thought the recording would settle any subsequent disputes about what was said (R. 84-88). He routinely carried a photography capable cell phone, although he did not use that capability (R. 106; File at 60). He attempted to record Mr. Harwig's counseling session on March 10, 2007; however, the device did not record the conversation for technical reasons (R. 88, 102-103; File at 60-61). He did not attempt to tape record the more intensive counseling session with Mr. Harwig on March 11, 2005 (R. 102-103). His cell phone did not contain any photographs, and his recording devices did not contain any other recordings of persons who did not consent to the recording prior to March 14, 2005 (R. 98-99; pg. 26).

On March 14, 2005, Appellant turned on the recording device in the parking lot and brought the recording device to his office area where he was arrested for stalking. The recording device captured the arresting officers telling Appellant he was under arrest (R. 90-91; File at 61). The officer who searched him, found a digital tape recorder, connected to a microphone, as well as two recording devices on Appellant's person (File at 136). Appellant's also had a cell phone with a photographic capability on his person (File at 60). Appellant denied that he possessed these devices in any rooms where the devices were prohibited (R. 130-131; File at 61).

SOR ¶¶ 1.g and 1.h allege Appellant brought these devices into a restricted area of a secure facility. He then recorded a conversation with his supervisor. The Command Security Manager, stated in an e-mail dated September 21, 2006, that Appellant admitted bringing a recording device into Room 506 of the Cude Building¹² and recording a conversation with his supervisor. She stated Room 506 in the Cude Building is a restricted area. She provided a copy of a Restricted sign.¹³ It includes the warning:

Photographing, making notes, drawings, maps, or graphic representations of this area or its activities is prohibited unless specifically authorized by the commanding officer. – Any such material found in the possession of unauthorized personnel will be confiscated.

¹² The Cude Building is Building 2592. See <http://www.dodtechmatch.com/DOD/Lab/ViewLab.aspx?id=20225>.

¹³ Appellant explained the sign she referenced was at the Guard desk, at Room 112-B, Building 2592 (R. 39-41). See pages 6 and 7 (sign & floor plan showing location of Room 112-B).

The sign does not preclude possession of photography or recording devices. The sign provides a general prohibition against collection of information pertaining to the physical security of an area, and against collection of classified information about other activities through making notes. For example, employees can certainly make notes as necessary of non-classified duties or purposes, but they are not permitted to make notes about the physical layout, security conditions or activities. Another sign applying only to "VISITORS" prohibits, "cameras . . . cellular telephones [, and] recorders." Appellant is an employee, not a visitor, and the visitor prohibition does not apply to him.

Appellant provided an exterior building photograph showing the locations of Building 2592 and 2592A (pg. 4). Essentially Building 2592 is a less restricted building in front of Building 2592A, which is a SKIF (R. 39-40). The Notice described above is posted at the Guard Desk in front of Building 2592.

There is a policy memorandum and standard operating procedure, which restrict or prohibit devices in particular rooms of Building 2592. ERDC Standard Operating Procedure (SOP) 190-13-1 prohibits recording devices and photographic devices in Building 2592A (pg. 8), and a small number of rooms in Building 2592 (pg. 8; R. 43). The rooms with restrictions are marked in yellow on the floor plan for Building 2592 (pg. 10). Restricted Area signs (pg. 9) are posted on doors of particular rooms in Building 2592 (R. 44-45; pg. 8-10). *See SOP, page 3; pg. 8).* Room 460 of Building 2592 is Mr. Harwig's office, and Room 442 is Appellant's office/cubical (R. 52; pg. 2, 11). These key locations are highlighted in yellow, and Room 460 is located in the ring closest to the center of the building (pg. 11). Room 442 is located directly across the hallway from Room 460 (pg. 11). Ms. Kennon's office is about 20 feet from Appellant's cubical.

A policy memorandum dated January 13, 2003, authorizes possession of cell phones and other personal electronic devices (PED) in Building 2592, but restricts their possession in areas where classified information is being discussed (R. 56; pg. 12-15).¹⁴ The Security Office is supposed to determine when the policy memorandum applies (pg. 14). Ten ERDC personnel signed the front of the policy memorandum indicating they were aware of the PED policy; however, Appellant did not sign the document (R. 56). Appellant said the PED policy was not part of his in-processing packet, and he did not see the PED policy until the middle of 2006 (R. 56-57). Appellant believed the persons signing the PED policy were guards (R. 57).

Appellant provided his route to his office and Mr. Harwig's office when carrying the PEDs (R. 92-95; pg. 10). The most direct route does not enter any areas where the possession of PEDs is prohibited (R. 94-95).

¹⁴ This is of course a reasonable restriction. Someone might have a conversation of a cell phone and inadvertently pick up a classified conversation, resulting in a security violation.

"[I]n Virginia it is not a criminal offense for a person to record a conversation where the person is a party to the communication or one of the parties to the communication has given prior consent to the recording. Va. Code § 19.2-62(B)(2). In other words, in Virginia, there is no criminal prohibition against recording a telephone conversation provided one of the parties to the conversation has consented to the recording." *United States v. Smallwood*, 365 F.Supp.2d 689, 697-698 (E.D. Va. 2005). After Army Regulation 600-20, paragraph 5-21 was rescinded in 1984, tape recording of conversations without consent of all parties was no longer prohibited by non-law enforcement¹⁵ personnel. See Clark, Wes, *Electronic Surveillance and Related Investigative Techniques*, 128 Mil.L.Rev. 155, 188-189 and n. 107 (Spring 1990). I was unable to locate any regulation or rule that Appellant violated when he tape recorded the officer arresting him, or when he attempted to tape record his supervisor's counseling session.

SOR ¶ 1.h (misrepresenting his address, and comments about making bombs)¹⁶

Appellant misrepresented his current legal address to his supervisory chain of command. SOR ¶ 1.h. His supervisor thought he lived in Kingstown rather than in Huntington Towers (File at 178). Appellant explained that the information about his address was accurate because he was in transition from an apartment to a house (File at 62-63).

SOR ¶ 1.h alleges Appellant made a veiled threat about his ability to make explosive devices (R. 83; File at 178). On March 11, 2005, Appellant told his supervisor that the explosives referred to were common high school projects (File at 63, 177). Appellant provided a detailed rebuttal to this allegation with references to supporting statements (File at 63-65).

CONCLUSIONS

As set forth in the regulation, every recommended personnel security decision must be a fair and impartial overall common sense decision based on all available evidence, both favorable and unfavorable. The decision must be arrived at by applying the standard that the grant or continuance of a security clearance or access to classified information is clearly within the interests of national security. Upon consideration of all the facts in evidence, and after application of all appropriate

¹⁵ Army Regulation 190-53, *Military Police Interception of Wire and Oral Communications for Law Enforcement Purposes* (November 3, 1986) includes an approval process for law enforcement tape recording with consent of one party. However, this regulation in paragraph 1-1 and 1-2a is made applicable to law enforcement activities and is not generally applicable to personnel such as Appellant.

¹⁶ See note 4, *supra*.

legal precepts, factors, and conditions, including those described briefly above, I conclude the following with respect to the allegations set forth in the SOR:

Security Violations

Under Guideline K, the Department of Defense is concerned that noncompliance "with security regulations raises doubt about an individual's trustworthiness, willingness, and ability to safeguard classified information."

There are two security violations disqualifying conditions (SV DC). SV DC 1 and 2 respectively provide, "unauthorized disclosure of classified information," and "violations that are deliberate or multiple or due to negligence." The evidence does not establish Appellant disclosed classified information, and/or violation of security rules.

Any of four security violations mitigating conditions (SV MC) could potentially mitigate security concerns. For SV MCs 1-3 to be applicable, the security violation must be inadvertent, isolated or infrequent, or due to improper or inadequate training. For SV MC 4 to apply, Applicant must demonstrate a positive attitude towards the discharge of security responsibilities. Assuming he violated a security rule, SV MCs 1-4 all apply. Appellant is a stickler for following the rules, and is very conscientious about following security rules. He is a devoted employee who is trustworthy and serious about security. He has a positive attitude towards security and has taken demonstrative and positive steps in discharging his security responsibilities.

Personal Conduct

Personal Conduct is always a security concern because it asks whether a person's past conduct justifies confidence the person can be trusted to properly safeguard classified information. Personal conduct involving questionable judgment, untrustworthiness, unreliability, lack of candor, dishonesty, or unwillingness to comply with rules and regulations could indicate that the person may not properly safeguard classified information.

I considered all Personal Conduct Disqualifying Conditions (PC DC), and PC DC 5 is potentially applicable, "a pattern of dishonesty or rules violations." As indicated previously, the record evidence did not establish violation of any rules.

I have considered all Personal Conduct Mitigating Conditions (PC MC), and PC MC 1, "The information was unsubstantiated or not pertinent to a determination of judgment, trustworthiness, or reliability," applies.

In all adjudications, the protection of our national security is the paramount concern. The objective of the security clearance process is the fair-minded,

FOR OFFICIAL USE ONLY
When unredacted this document contains information
EXEMPT FROM MANDATORY DISCLOSURE under the FOIA
Exemption 6 applies

commonsense assessment of a person's life to make an affirmative determination that the person is eligible for a security clearance. Indeed the adjudicative process is a careful weighing of a number of variables in considering the "whole person" concept. It recognizes that we should view a person by the totality of his or her acts, omissions, motivations and various other variables. Each case must be adjudged on its own merits, taking into consideration all relevant circumstances, and applying sound judgment, mature thinking, and careful analysis.

I have also considered the following specific factors: the nature and seriousness of the conduct and surrounding circumstances, to include knowledgeable participation; the frequency and recency of the conduct; the individual's age and maturity at the time of the conduct; the voluntariness of participation; the presence or absence of rehabilitation and other pertinent behavioral changes; the motivation for the conduct; the potential for pressure, coercion, exploitation, or duress; and the likelihood of continuation or recurrence of the conduct.

Having considered the "whole person" concept in evaluating Appellant's risk and vulnerability in protecting our national interests, I find Appellant has refuted the allegations of security violations. Even if he failed to refute the allegations, he successfully mitigated the security concerns raised by the alleged security violations and personal conduct security concerns. I am persuaded by the totality of the evidence in this case that it is clearly consistent with the interests of national security to grant Appellant a security clearance.

FORMAL FINDINGS

SECURITY VIOLATIONS: For Appellant
PERSONAL CONDUCT: For Appellant

RECOMMENDED DECISION

In reaching my decision, I have considered the entire record and have applied the appropriate AGs contained in DoD Regulation 5200.2, as amended. Since the protection of the national security is the paramount consideration, the final decision in each case is arrived at by applying the standard that doubt concerning personnel being considered for access to classified information will be resolved in favor of national security. In light of all of the information in this case, it is clearly consistent with the interests of national security to overturn the letter revoking his eligibility for access to SCI information and his access to classified information.

Mark W. Harvey
Mark W. Harvey

Administrative Judge

FOR OFFICIAL USE ONLY
When unredacted this document contains information
EXEMPT FROM MANDATORY DISCLOSURE under the FOIA
Exemption 6 applies



The Age Discrimination in Employment Act of 1967

EDITOR'S NOTE: The following is the text of the Age Discrimination in Employment Act of 1967 (Pub. L. 90-202) (ADEA), as amended, as it appears in volume 29 of the United States Code, beginning at section 621. The ADEA prohibits employment discrimination against persons 40 years of age or older. The Older Workers Benefit Protection Act (Pub. L. 101-433) amended several sections of the ADEA. In addition, section 115 of the Civil Rights Act of 1991 (P.L. 102-166) amended section 7(e) of the ADEA (29 U. S.C. 626(e)). Cross references to the ADEA as enacted appear in italics following each section heading. Editor's notes also appear in italics.

An Act

To prohibit age discrimination in employment.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, that this Act may be cited as the "Age Discrimination in Employment Act of 1967."

CONGRESSIONAL STATEMENT OF FINDINGS AND PURPOSE

SEC. 621. [Section 2]

(a) The Congress hereby finds and declares that-

- (1) in the face of rising productivity and affluence, older workers find themselves disadvantaged in their efforts to retain employment, and especially to regain employment when displaced from jobs;
- (2) the setting of arbitrary age limits regardless of potential for job performance has become a common practice, and certain otherwise desirable practices may work to the disadvantage of older persons;

transferred to a supervisory or administrative position. For the purpose of this subsection, "detention" includes the duties of employees assigned to guard individuals incarcerated in any penal institution.

(l) The term "compensation, terms, conditions, or privileges of employment" encompasses all employee benefits, including such benefits provided pursuant to a bona fide employee benefit plan.

AGE LIMITS

SEC. 631. *[Section 12]*

(a) Individuals of at least 40 years of age

The prohibitions in this chapter shall be limited to individuals who are at least 40 years of age.

(b) Employees or applicants for employment in Federal Government

In the case of any personnel action affecting employees or applicants for employment which is subject to the provisions of section 633a of this title *[section 15]*, the prohibitions established in section 633a of this title *[section 15]* shall be limited to individuals who are at least 40 years of age.

(c) Bona fide executives or high policymakers

(1) Nothing in this chapter shall be construed to prohibit compulsory retirement of any employee who has attained 65 years of age and who, for the 2-year period immediately before retirement, is employed in a bona fide executive or a high policymaking position, if such employee is entitled to an immediate nonforfeitable annual retirement benefit from a pension, profit-sharing, savings, or deferred compensation plan, or any combination of such plans, of the employer of such employee, which equals, in the aggregate, at least \$44,000.

(2) In applying the retirement benefit test of paragraph (1) of this subsection, if any such retirement benefit is in a form other than a straight life annuity (with no ancillary benefits), or if employees contribute to any such plan or make rollover contributions, such benefit shall be adjusted in accordance with regulations prescribed by the Equal Employment Opportunity Commission, after consultation with the Secretary of the Treasury, so that the benefit is the equivalent of a straight life annuity (with no ancillary benefits) under a plan to which employees do not contribute and under which no rollover contributions are made.

ANNUAL REPORT

SEC. 632. [Section 13]

[Repealed]

FEDERAL-STATE RELATIONSHIP

SEC. 633. [Section 14]

(a) Federal action superseding State action

Nothing in this chapter shall affect the jurisdiction of any agency of any State performing like functions with regard to discriminatory employment practices on account of age except that upon commencement of action under this chapter such action shall supersede any State action.

(b) Limitation of Federal action upon commencement of State proceedings

In the case of an alleged unlawful practice occurring in a State which has a law prohibiting discrimination in employment because of age and establishing or authorizing a State authority to grant or seek relief from such discriminatory practice, no suit may be brought under section 626 of this title [section 7] before the expiration of sixty days after proceedings have been commenced under the State law, unless such proceedings have been earlier terminated: *Provided*, That such sixty-day period shall be extended to one hundred and twenty days during the first year after the effective date of such State law. If any requirement for the commencement of such proceedings is imposed by a State authority other than a requirement of the filing of a written and signed statement of the facts upon which the proceeding is based, the proceeding shall be deemed to have been commenced for the purposes of this subsection at the time such statement is sent by registered mail to the appropriate State authority.

NONDISCRIMINATION ON ACCOUNT OF AGE IN FEDERAL GOVERNMENT EMPLOYMENT

SEC. 633a. [Section 15]

(a) Federal agencies affected

All personnel actions affecting employees or applicants for employment who are at least 40 years of age (except personnel actions with regard to aliens employed outside the limits of the United States)

in military departments as defined in section 102 of Title 5 [5 U.S.C. § 102], in executive agencies as defined in section 105 of Title 5 [5 U.S.C. § 105] (including employees and applicants for employment who are paid from nonappropriated funds), in the United States Postal Service and the Postal Regulatory Commission, in those units in the government of the District of Columbia having positions in the competitive service, and in those units of the judicial branch of the Federal Government having positions in the competitive service, in the Smithsonian Institution, and in the Government Printing Office, the Government Accountability Office, and the Library of Congress shall be made free from any discrimination based on age.

(b) Enforcement by Equal Employment Opportunity Commission and by Librarian of Congress in the Library of Congress; remedies; rules, regulations, orders, and instructions of Commission: compliance by Federal agencies; powers and duties of Commission; notification of final action on complaint of discrimination; exemptions: bona fide occupational qualification

Except as otherwise provided in this subsection, the Equal Employment Opportunity Commission is authorized to enforce the provisions of subsection (a) of this section through appropriate remedies, including reinstatement or hiring of employees with or without backpay, as will effectuate the policies of this section. The Equal Employment Opportunity Commission shall issue such rules, regulations, orders, and instructions as it deems necessary and appropriate to carry out its responsibilities under this section. The Equal Employment Opportunity Commission shall-

- (1) be responsible for the review and evaluation of the operation of all agency programs designed to carry out the policy of this section, periodically obtaining and publishing (on at least a semiannual basis) progress reports from each department, agency, or unit referred to in subsection (a) of this section;
- (2) consult with and solicit the recommendations of interested individuals, groups, and organizations relating to nondiscrimination in employment on account of age; and
- (3) provide for the acceptance and processing of complaints of discrimination in Federal employment on account of age.

The head of each such department, agency, or unit shall comply with such rules, regulations, orders, and instructions of the Equal Employment Opportunity Commission which shall include a provision that an employee or applicant for employment shall be notified of any final action taken on any complaint of discrimination filed by him thereunder. Reasonable exemptions to the provisions of this section may be established by the Commission but only when the Commission has established a maximum age requirement on the basis of a determination that age is a bona fide occupational qualification necessary to the performance of the duties of the position. With respect to employment in the Library of Congress, authorities granted in this subsection to the Equal Employment Opportunity Commission shall be exercised by the Librarian of Congress.

(c) Civil actions; jurisdiction; relief

Any person aggrieved may bring a civil action in any Federal district court of competent jurisdiction for such legal or equitable relief as will effectuate the purposes of this chapter.

(d) Notice to Commission; time of notice; Commission notification of prospective defendants; Commission elimination of unlawful practices

When the individual has not filed a complaint concerning age discrimination with the Commission, no civil action may be commenced by any individual under this section until the individual has given the Commission not less than thirty days' notice of an intent to file such action. Such notice shall be filed within one hundred and eighty days after the alleged unlawful practice occurred. Upon receiving a notice of intent to sue, the Commission shall promptly notify all persons named therein as prospective defendants in the action and take any appropriate action to assure the elimination of any unlawful practice.

(e) Duty of Government agency or official

Nothing contained in this section shall relieve any Government agency or official of the responsibility to assure nondiscrimination on account of age in employment as required under any provision of Federal law.

(f) Applicability of statutory provisions to personnel action of Federal departments, etc.

Any personnel action of any department, agency, or other entity referred to in subsection (a) of this section shall not be subject to, or affected by, any provision of this chapter, other than the provisions of sections 7(d)(3) and 631(b) of this title [*section 12(b)*] and the provisions of this section.

(g) Study and report to President and Congress by Equal Employment Opportunity Commission; scope

(1) The Equal Employment Opportunity Commission shall undertake a study relating to the effects of the amendments made to this section by the Age Discrimination in Employment Act Amendments of 1978, and the effects of section 631(b) of this title [*section 12(b)*].

(2) The Equal Employment Opportunity Commission shall transmit a report to the President and to the Congress containing the findings of the Commission resulting from the study of the Commission under paragraph (1) of this subsection. Such report shall be transmitted no later than January 1, 1980.

EFFECTIVE DATE

[Section 16 of the ADEA (not reproduced in the U.S. Code)]

This Act shall become effective one hundred and eighty days after enactment, except (a) that the Secretary of Labor may extend the delay in effective date of any provision of this Act up to an additional ninety days thereafter if he finds that such time is necessary in permitting adjustments to the provisions hereof, and (b) that on or after the date of enactment the EEOC [originally, the Secretary of Labor] is authorized to issue such rules and regulations as may be necessary to carry out its provisions.

AUTHORIZATION OF APPROPRIATIONS

SEC. 634. *[Section 17]*

There are hereby authorized to be appropriated such sums as may be necessary to carry out this chapter



Title VII of the Civil Rights Act of 1964

EDITOR'S NOTE: The following is the text of Title VII of the Civil Rights Act of 1964 (Pub. L. 88-352) (Title VII), as amended, as it appears in volume 42 of the United States Code, beginning at section 2000e. Title VII prohibits employment discrimination based on race, color, religion, sex and national origin. The Civil Rights Act of 1991 (Pub. L. 102-166) (CRA) and the Lily Ledbetter Fair Pay Act of 2009 (Pub. L. 111-2) amend several sections of Title VII. In addition, section 102 of the CRA (which is printed elsewhere in this publication) amends the Revised Statutes by adding a new section following section 1977 (42 U.S.C. 1981), to provide for the recovery of compensatory and punitive damages in cases of intentional violations of Title VII, the Americans with Disabilities Act of 1990, and section 501 of the Rehabilitation Act of 1973. Cross references to Title VII as enacted appear in italics following each section heading. Editor's notes also appear in italics.

An Act

To enforce the constitutional right to vote, to confer jurisdiction upon the district courts of the United States to provide injunctive relief against discrimination in public accommodations, to authorize the attorney General to institute suits to protect constitutional rights in public facilities and public education, to extend the Commission on Civil Rights, to prevent discrimination in federally assisted programs, to establish a Commission on Equal Employment Opportunity, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, That this Act may be cited as the "Civil Rights Act of 1964".

DEFINITIONS

SEC. 2000e. [Section 701]

For the purposes of this subchapter-

[Original text: (a) This title shall become effective one year after the date of its enactment.

(b) Notwithstanding subsection (a), sections of this title other than sections 703, 704, 706, and 707 shall become effective immediately.

(c)] The President shall, as soon as feasible after July 2, 1964 [the date of enactment of this title], convene one or more conferences for the purpose of enabling the leaders of groups whose members will be affected by this subchapter to become familiar with the rights afforded and obligations imposed by its provisions, and for the purpose of making plans which will result in the fair and effective administration of this subchapter when all of its provisions become effective. The President shall invite the participation in such conference or conferences of (1) the members of the President's Committee on Equal Employment Opportunity, (2) the members of the Commission on Civil Rights, (3) representatives of State and local agencies engaged in furthering equal employment opportunity, (4) representatives of private agencies engaged in furthering equal employment opportunity, and (5) representatives of employers, labor organizations, and employment agencies who will be subject to this subchapter.

TRANSFER OF AUTHORITY

[Enforcement of Section 717 was transferred to the Equal Employment Opportunity Commission from the Civil Service Commission (Office of Personnel Management) effective January 1, 1979 under the President's Reorganization Plan No. 1 of 1978.]

EMPLOYMENT BY FEDERAL GOVERNMENT

SEC. 2000e-16. *[Section 717]*

(a) Discriminatory practices prohibited; employees or applicants for employment subject to coverage
All personnel actions affecting employees or applicants for employment (except with regard to aliens employed outside the limits of the United States) in military departments as defined in section 102 of Title 5 *[United States Code]*, in executive agencies *[originally, other than the General Accounting Office]* as defined in section 105 of Title 5 *[United States Code]* (including employees and applicants for employment who are paid from nonappropriated funds), in the United States Postal Service and the Postal Regulatory Commission, in those units of the Government of the District of Columbia having positions in the competitive service, and in those units of the judicial branch of the Federal Government having positions in the competitive service, in the Smithsonian Institution, and in the

Government Printing Office, the Government Accountability Office, and the Library of Congress shall be made free from any discrimination based on race, color, religion, sex, or national origin.

(b) Equal Employment Opportunity Commission; enforcement powers; issuance of rules, regulations, etc.; annual review and approval of national and regional equal employment opportunity plans; review and evaluation of equal employment opportunity programs and publication of progress reports; consultations with interested parties; compliance with rules, regulations, etc.; contents of national and regional equal employment opportunity plans; authority of Librarian of Congress

Except as otherwise provided in this subsection, the Equal Employment Opportunity Commission [*originally, Civil Service Commission*] shall have authority to enforce the provisions of subsection (a) of this section through appropriate remedies, including reinstatement or hiring of employees with or without back pay, as will effectuate the policies of this section, and shall issue such rules, regulations, orders and instructions as it deems necessary and appropriate to carry out its responsibilities under this section. The Equal Employment Opportunity Commission [*originally, Civil Service Commission*] shall-

- (1) be responsible for the annual review and approval of a national and regional equal employment opportunity plan which each department and agency and each appropriate unit referred to in subsection (a) of this section shall submit in order to maintain an affirmative program of equal employment opportunity for all such employees and applicants for employment;
- (2) be responsible for the review and evaluation of the operation of all agency equal employment opportunity programs, periodically obtaining and publishing (on at least a semiannual basis) progress reports from each such department, agency, or unit; and
- (3) consult with and solicit the recommendations of interested individuals, groups, and organizations relating to equal employment opportunity.

The head of each such department, agency, or unit shall comply with such rules, regulations, orders, and instructions which shall include a provision that an employee or applicant for employment shall be notified of any final action taken on any complaint of discrimination filed by him thereunder. The plan submitted by each department, agency, and unit shall include, but not be limited to-

- (1) provision for the establishment of training and education programs designed to provide a maximum opportunity for employees to advance so as to perform at their highest potential; and
- (2) a description of the qualifications in terms of training and experience relating to equal employment opportunity for the principal and operating officials of each such department, agency, or unit responsible for carrying out the equal employment

opportunity program and of the allocation of personnel and resources proposed by such department, agency, or unit to carry out its equal employment opportunity program.

With respect to employment in the Library of Congress, authorities granted in this subsection to the Equal Employment Opportunity Commission [*originally, Civil Service Commission*] shall be exercised by the Librarian of Congress.

(c) Civil action by employee or applicant for employment for redress of grievances; time for bringing of action; head of department, agency, or unit as defendant

Within 90 days of receipt of notice of final action taken by a department, agency, or unit referred to in subsection (a) of this section, or by the Equal Employment Opportunity Commission [*originally, Civil Service Commission*] upon an appeal from a decision or order of such department, agency, or unit on a complaint of discrimination based on race, color, religion, sex or national origin, brought pursuant to subsection (a) of this section, Executive Order 11478 or any succeeding Executive orders, or after one hundred and eighty days from the filing of the initial charge with the department, agency, or unit or with the Equal Employment Opportunity Commission [*originally, Civil Service Commission*] on appeal from a decision or order of such department, agency, or unit until such time as final action may be taken by a department, agency, or unit, an employee or applicant for employment, if aggrieved by the final disposition of his complaint, or by the failure to take final action on his complaint, may file a civil action as provided in section 2000e-5 of this title [*section 706*], in which civil action the head of the department, agency, or unit, as appropriate, shall be the defendant.

(d) Section 2000e-5(f) through (k) of this title applicable to civil actions

The provisions of section 2000e-5(f) through (k) of this title [*section 706(f) through (k)*], as applicable, shall govern civil actions brought hereunder, and the same interest to compensate for delay in payment shall be available as in cases involving nonpublic parties.

(e) Government agency or official not relieved of responsibility to assure nondiscrimination in employment or equal employment opportunity

Nothing contained in this Act shall relieve any Government agency or official of its or his primary responsibility to assure nondiscrimination in employment as required by the Constitution and statutes or of its or his responsibilities under Executive Order 11478 relating to equal employment opportunity in the Federal Government.

(f) Section 2000e-5(e)(3) [*Section 706(e)(3)*] shall apply to complaints of discrimination in compensation under this section.

(8) Of the total number of final agency actions rendered in such fiscal year involving a finding of discrimination

(A) the number and percentage involving a finding of discrimination based on each of the respective bases of alleged discrimination, and

(B) of the number specified under subparagraph (A) for each of the respective bases of alleged discrimination

(i) the number and percentage that were rendered without a hearing before an administrative judge of the Equal Employment Opportunity Commission, and

(ii) the number and percentage that were rendered after a hearing before an administrative judge of the Equal Employment Opportunity Commission.

(9) Of the total number of final agency actions rendered in such fiscal year involving a finding of discrimination

(A) the number and percentage involving a finding of discrimination in connection with each of the respective issues of alleged discrimination, and

(B) of the number specified under subparagraph (A) for each of the respective issues of alleged discrimination

(i) the number and percentage that were rendered without a hearing before an administrative judge of the Equal Employment Opportunity Commission, and

(ii) the number and percentage that were rendered after a hearing before an administrative judge of the Equal Employment Opportunity Commission.

(10)(A) Of the total number of complaints pending in such fiscal year (as described in the parenthetical matter in paragraph (6)), the number that were first filed before the start of the then current fiscal year.

(B) With respect to those pending complaints that were first filed before the start of the then current fiscal year

(i) the number of individuals who filed those complaints, and

(ii) the number of those complaints which are at the various steps of the complaint process.

(C) Of the total number of complaints pending in such fiscal year (as described in the parenthetical matter in paragraph (6)), the total number of complaints with respect to which the agency violated the requirements of section 1614.106(e)(2) of title 29 of the Code of Federal Regulations (as in effect on July 1, 2000, and amended from time to time) by failing to conduct within 180 days of the filing of such complaints an impartial and appropriate investigation of such complaints.

(c) TIMING AND OTHER REQUIREMENTS.

(1) CURRENT YEAR DATA. Data posted under this section for the then current fiscal year shall include both

(A) interim year-to-date data, updated quarterly, and

(B) final year-end data.

(2) DATA FOR PRIOR YEARS. The data posted by a Federal agency under this section for a fiscal year (both interim and final) shall include, for each item under subsection (b), such agency's corresponding year-end data for each of the 5 immediately preceding fiscal years (or, if not available for all 5 fiscal years, for however many of those 5 fiscal years for which data are available).

SEC. 302. DATA TO BE POSTED BY THE EQUAL EMPLOYMENT OPPORTUNITY COMMISSION.

(a) IN GENERAL. The Equal Employment Opportunity Commission shall post on its public Web site, in the time, form, and manner prescribed under section 303 for purposes of this section, summary statistical data relating to

(1) hearings requested before an administrative judge of the Commission on complaints described in section 301, and

(2) appeals filed with the Commission from final agency actions on complaints described in section 301.

(b) SPECIFIC REQUIREMENTS. The data posted under this section shall, with respect to the hearings and appeals described in subsection (a), include summary statistical data corresponding to that described in paragraphs (1) through (10) of section 301(b), and shall be subject to the same timing and other requirements as set forth in section 301(c).

(c) COORDINATION. The data required under this section shall be in addition to the data the Commission is required to post under section 301 as an employing Federal agency.

SEC. 303. RULES.

The Equal Employment Opportunity Commission shall issue any rules necessary to carry out this title.

[For abolition of Immigration and Naturalization Service, transfer of functions, and treatment of related references, see note set out under section 1551 of Title 8, Aliens and Nationality.]

[For transfer of authorities, functions, personnel, and assets of the Bureau of Alcohol, Tobacco and Firearms, including the related functions of the Secretary of the Treasury, to the Department of Justice, see section 531(c) of Title 6, Domestic Security, and section 599A(c)(1) of Title 28, Judiciary and Judicial Procedure.]

[Memorandum of President of the United States, July 8, 2003, 68 F.R. 45155, delegated to Director of Office of Personnel Management authority of President under section 204(a) of Public Law 107-174, set out above.]

§ 2302. Prohibited personnel practices

(a)(1) For the purpose of this title, prohibited personnel practice means any action described in subsection (b).

(2) For the purpose of this section

(A) personnel action means

(i) an appointment;

(ii) a promotion;

(iii) an action under chapter 75 of this title or other disciplinary or corrective action;

(iv) a detail, transfer, or reassignment;

(v) a reinstatement;

(vi) a restoration;

(vii) a reemployment;

(viii) a performance evaluation under chapter 43 of this title;

(ix) a decision concerning pay, benefits, or awards, or concerning education or training if the education or training may reasonably be expected to lead to an appointment, promotion, performance evaluation, or other action described in this subparagraph;

(x) a decision to order psychiatric testing or examination; and

(xi) any other significant change in duties, responsibilities, or working conditions;

with respect to an employee in, or applicant for, a covered position in an agency, and in the case of an alleged prohibited personnel practice described in subsection (b)(8), an employee or applicant for employment in a Government corporation as defined in section 9101 of title 31;

(B) covered position means, with respect to any personnel action, any position in the competitive service, a career appointee position in the Senior Executive Service, or a position in the excepted service, but does not include any position which is, prior to the personnel action

(1) excepted from the competitive service because of its confidential, policy-determining, policy-making, or policy-advocating character; or

(ii) excluded from the coverage of this section by the President based on a determination by the President that it is necessary and warranted by conditions of good administration; and

(C) agency means an Executive agency and the Government Printing Office, but does not include

(i) a Government corporation, except in the case of an alleged prohibited personnel practice described under subsection (b)(8);

(ii) the Federal Bureau of Investigation, the Central Intelligence Agency, the Defense Intelligence Agency, the National Geospatial-Intelligence Agency, the National Security Agency, and, as determined by the President, any Executive agency or unit thereof the principal function of which is the conduct of foreign intelligence or counterintelligence activities; or

(iii) the Government Accountability Office.

(b) Any employee who has authority to take, direct others to take, recommend, or approve any personnel action, shall not, with respect to such authority

(1) discriminate for or against any employee or applicant for employment

(A) on the basis of race, color, religion, sex, or national origin, as prohibited under section 717 of the Civil Rights Act of 1964 (42 U.S.C. 2000e 16);

(B) on the basis of age, as prohibited under sections 12 and 15 of the Age Discrimination in Employment Act of 1967 (29 U.S.C. 631, 633a);

(C) on the basis of sex, as prohibited under section 6(d) of the Fair Labor Standards Act of 1938 (29 U.S.C. 206(d));

(D) on the basis of handicapping condition, as prohibited under section 501 of the Rehabilitation Act of 1973 (29 U.S.C. 791); or

(E) on the basis of marital status or political affiliation, as prohibited under any law, rule, or regulation;

(2) solicit or consider any recommendation or statement, oral or written, with respect to any individual who requests or is under consideration for any personnel action unless such recommendation or statement is based on the personal knowledge or records of the person furnishing it and consists of

(A) an evaluation of the work performance, ability, aptitude, or general qualifications of such individual; or

(B) an evaluation of the character, loyalty, or suitability of such individual;

(3) coerce the political activity of any person (including the providing of any political contribution or service), or take any action against any employee or applicant for employment as a reprisal for the refusal of any person to engage in such political activity;

(4) deceive or willfully obstruct any person with respect to such person's right to compete for employment;

(5) influence any person to withdraw from competition for any position for the purpose of improving or injuring the prospects of any other person for employment;

(6) grant any preference or advantage not authorized by law, rule, or regulation to any employee or applicant for employment (including defining the scope or manner of competition or the requirements for any position) for the purpose of improving or injuring the prospects of any particular person for employment;

(7) appoint, employ, promote, advance, or advocate for appointment, employment, promotion, or advancement, in or to a civilian position any individual who is a relative (as defined in section 3110(a)(3) of this title) of such employee if such position is in the agency in which such employee is serving as a public official (as defined in section 3110(a)(2) of this title) or over which such employee exercises jurisdiction or control as such an official;

(8) take or fail to take, or threaten to take or fail to take, a personnel action with respect to any employee or applicant for employment because of

(A) any disclosure of information by an employee or applicant which the employee or applicant reasonably believes evidences

(i) a violation of any law, rule, or regulation, or

(ii) gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety,

if such disclosure is not specifically prohibited by law and if such information is not specifically required by Executive order to be kept secret in the interest of national defense or the conduct of foreign affairs; or

(B) any disclosure to the Special Counsel, or to the Inspector General of an agency or another employee designated by the head of the agency to receive such disclosures, of information which the employee or applicant reasonably believes evidences

(i) a violation of any law, rule, or regulation, or

(ii) gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety;

(9) take or fail to take, or threaten to take or fail to take, any personnel action against any employee or applicant for employment because of

(A) the exercise of any appeal, complaint, or grievance right granted by any law, rule, or regulation;

(B) testifying for or otherwise lawfully assisting any individual in the exercise of any right referred to in subparagraph (A);

(C) cooperating with or disclosing information to the Inspector General of an agency, or the Special Counsel, in accordance with applicable provisions of law; or

(D) for¹ refusing to obey an order that would require the individual to violate a law;

¹So in original. The word for probably should not appear.

(10) discriminate for or against any employee or applicant for employment on the basis of conduct which does not adversely affect the performance of the employee or applicant or the performance of others; except that nothing in this paragraph shall prohibit an agency from taking into account in determining suitability or fitness any conviction of the employee or applicant for any crime under the laws of any State, of the District of Columbia, or of the United States;

(11)(A) knowingly take, recommend, or approve any personnel action if the taking of such action would violate a veterans preference requirement; or

(B) knowingly fail to take, recommend, or approve any personnel action if the failure to take such action would violate a veterans preference requirement; or

(12) take or fail to take any other personnel action if the taking of or failure to take such action violates any law, rule, or regulation implementing, or directly concerning, the merit system principles contained in section 2301 of this title.

This subsection shall not be construed to authorize the withholding of information from the Congress or the taking of any personnel action against an employee who discloses information to the Congress.

(c) The head of each agency shall be responsible for the prevention of prohibited personnel practices, for the compliance with and enforcement of applicable civil service laws, rules, and regulations, and other aspects of personnel management, and for ensuring (in consultation with the Office of Special Counsel) that agency employees are informed of the rights and remedies available to them under this chapter and chapter 12 of this title. Any individual to whom the head of an agency delegates authority for personnel management, or for any aspect thereof, shall be similarly responsible within the limits of the delegation.

(d) This section shall not be construed to extinguish or lessen any effort to achieve equal employment opportunity through affirmative action or any right or remedy available to any employee or applicant for employment in the civil service under

(1) section 717 of the Civil Rights Act of 1964 (42 U.S.C. 2000e-16), prohibiting discrimination on the basis of race, color, religion, sex, or national origin;

(2) sections 12 and 15 of the Age Discrimination in Employment Act of 1967 (29 U.S.C. 631, 633a), prohibiting discrimination on the basis of age;

(3) under section 6(d) of the Fair Labor Standards Act of 1938 (29 U.S.C. 206(d)), prohibiting discrimination on the basis of sex;

(4) section 501 of the Rehabilitation Act of 1973 (29 U.S.C. 791), prohibiting discrimination on the basis of handicapping condition; or

(5) the provisions of any law, rule, or regulation prohibiting discrimination on the basis of marital status or political affiliation.

(e)(1) For the purpose of this section, the term veterans preference requirement means any of the following provisions of law:

(A) Sections 2108, 3305(b), 3309, 3310, 3311, 3312, 3313, 3314, 3315, 3316, 3317(b), 3318, 3320, 3351, 3352, 3363, 3501, 3502(b), 3504, and 4303(e) and (with respect to a preference eligible referred to in section 7511(a)(1)(B)) subchapter II of chapter 75 and section 7701.

(B) Sections 943(c)(2) and 1784(c) of title 10.

(C) Section 1308(b) of the Alaska National Interest Lands Conservation Act.

(D) Section 301(c) of the Foreign Service Act of 1980.

(E) Sections 106(f),² 7281(e), and 7802(5)² of title 38.

(F) Section 1005(a) of title 39.

(G) Any other provision of law that the Director of the Office of Personnel Management designates in regulations as being a veterans preference requirement for the purposes of this subsection.

(H) Any regulation prescribed under subsection (b) or (c) of section 1302 and any other regulation that implements a provision of law referred to in any of the preceding subparagraphs.

(2) Notwithstanding any other provision of this title, no authority to order corrective action shall be available in connection with a prohibited personnel practice described in subsection (b)(11). Nothing in this paragraph shall be considered to affect any authority under section 1215 (relating to disciplinary action).

(Added Pub. L. 95-454, title I, § 101(a), Oct. 13, 1978, 92 Stat. 1114; amended Pub. L. 101-12, § 4, Apr. 10, 1989, 103 Stat. 32; Pub. L. 101-474, § 5(d), Oct. 30, 1990, 104 Stat. 1099; Pub. L. 102-378, § 2(5), Oct. 2, 1992, 106 Stat. 1346; Pub. L. 103-94, § 8(c), Oct. 6, 1993, 107 Stat. 1007; Pub. L. 103-359, title V, § 501(c), Oct. 14, 1994, 108 Stat. 3429; Pub. L. 103-424, § 5, Oct. 29, 1994, 108 Stat. 4363; Pub. L. 104-197, title III, § 315(b)(2), Sept. 16, 1996, 110 Stat. 2416, Pub. L. 104-201, div. A, title XI, § 1122(a)(1), title XVI, § 1615(b), Sept. 23, 1996, 110 Stat. 2687, 2741; Pub. L. 105-339, § 6(a), (b), (c)(2), Oct. 31, 1998, 112 Stat. 3187, 3188; Pub. L. 108-271, § 8(b), July 7, 2004, 118 Stat. 814; Pub. L. 110-417, [div. A], title IX, § 931(a)(1), Oct. 14, 2008, 122 Stat. 4575.)

REFERENCES IN TEXT

Section 1308(b) of the Alaska National Interest Lands Conservation Act, referred to in subsec. (e)(1)(C), is classified to section 3198(b) of Title 16, Conservation.

Section 301(c) of the Foreign Service Act of 1980, referred to in subsec. (e)(1)(D), is classified to section 3941(c) of Title 22, Foreign Relations and Intercourse.

Section 106(f) of title 38, referred to in subsec. (e)(1)(E), was enacted subsequent to the enactment of subsec. (e) of this section.

Section 7802(5) of title 38, referred to in subsec. (e)(1)(E), was redesignated section 7802(e) of title 38 by Pub. L. 108-170, title III, § 304(b)(3), Dec. 6, 2003, 117 Stat. 2059.

AMENDMENTS

2008 Subsec. (a)(2)(C)(ii). Pub. L. 110-417 substituted National Geospatial-Intelligence Agency for National Imagery and Mapping Agency.

2004 Subsec. (a)(2)(C)(iii). Pub. L. 108-271 substituted Government Accountability Office for General Accounting Office.

²See References in Text note below.

1998 Subsec. (a)(1). Pub. L. 105-339, § 6(c)(2), amended par. (1) generally. Prior to amendment, par. (1) read as follows: For purposes of this title, prohibited personnel practice means the following:

(A) Any action described in subsection (b) of this section.

(B) Any action or failure to act that is designated as a prohibited personnel action under section 1599c(a) of title 10.

Subsec. (b)(10) to (12). Pub. L. 105-339, § 6(a), struck out or at end of par. (10), added par. (11), and redesignated former par. (11) as (12).

Subsec. (e). Pub. L. 105-339, § 6(b), added subsec. (e).

1996 Subsec. (a)(1). Pub. L. 104-201, § 1615(b), amended par. (1) generally. Prior to amendment, par. (1) read as follows: For the purpose of this title, prohibited personnel practice means any action described in subsection (b) of this section.

Subsec. (a)(2)(C)(ii). Pub. L. 104-201, § 1122(a)(1), substituted National Imagery and Mapping Agency for Central Imagery Office.

Subsec. (b)(2). Pub. L. 104-197 amended par. (2) generally. Prior to amendment, par. (2) read as follows: solicit or consider any recommendation or statement, oral or written, with respect to any individual who requests or is under consideration for any personnel action except as provided under section 3303(f).

1994 Subsec. (a)(2)(A). Pub. L. 103-424, § 5(a)(3), in concluding provisions, inserted before semicolon, and in the case of an alleged prohibited personnel practice described in subsection (b)(8), an employee or applicant for employment in a Government corporation as defined in section 9101 of title 31.

Subsec. (a)(2)(A)(x), (xi). Pub. L. 103-424, § 5(a)(1), (2), added cl. (x) and (xi) and struck out former cl. (x) which read as follows: any other significant change in duties or responsibilities which is inconsistent with the employee's salary or grade level.

Subsec. (a)(2)(B). Pub. L. 103-424, § 5(b), amended subpar. (B) generally. Prior to amendment, subpar. (B) read as follows: covered position means any position in the competitive service, a career appointee position in the Senior Executive Service, or a position in the excepted service, but does not include

(i) a position which is excepted from the competitive service because of its confidential, policy-determining, policy-making, or policy-advocating character; or

(ii) any position excluded from the coverage of this section by the President based on a determination by the President that it is necessary and warranted by conditions of good administration.

Subsec. (a)(2)(C)(i). Pub. L. 103-424, § 5(c), inserted before semicolon, except in the case of an alleged prohibited personnel practice described under subsection (b)(8).

Subsec. (a)(2)(C)(ii). Pub. L. 103-359 inserted the Central Imagery Office, after Defense Intelligence Agency.

Subsec. (c). Pub. L. 103-424, § 5(d), inserted before period at end of first sentence, and for ensuring (in consultation with the Office of Special Counsel) that agency employees are informed of the rights and remedies available to them under this chapter and chapter 12 of this title.

1993 Subsec. (b)(2). Pub. L. 103-94 amended par. (2) generally. Prior to amendment, par. (2) read as follows: solicit or consider any recommendation or statement, oral or written, with respect to any individual who requests or is under consideration for any personnel action unless such recommendation or statement is based on the personal knowledge or records of the person furnishing it and consists of

(A) an evaluation of the work performance, ability, aptitude, or general qualifications of such individual; or

(B) an evaluation of the character, loyalty, or suitability of such individual.

1992 Subsec. (b)(8)(B). Pub. L. 102-378 substituted Special Counsel for Special Counsel of the Merit Systems Protection Board.

1990 Subsec. (a)(2)(C). Pub. L. 101-474 struck out, the Administrative Office of the United States Courts, after means an Executive agency.

1989 Subsec. (b)(8). Pub. L. 101-12, § 4(a), in introductory provision inserted, or threaten to take or fail to take, after fail to and substituted because of for as a reprisal for, in subparagraph (A) substituted any disclosure for a disclosure, in subparagraph (A)(ii) inserted gross before mismanagement, in subparagraph (B) substituted any disclosure for a disclosure, and in subparagraph (B)(ii) inserted gross before mismanagement.

Subsec. (b)(9). Pub. L. 101-12, § 4(b), amended par. (9) generally. Prior to amendment, par. (9) read as follows: take or fail to take any personnel action against any employee or applicant for employment as a reprisal for the exercise of any appeal right granted by any law, rule, or regulation; .

EFFECTIVE DATE OF 1996 AMENDMENTS

Amendment by section 1122(a)(1) of Pub. L. 104-201 effective Oct. 1, 1996, see section 1124 of Pub. L. 104-201, set out as a note under section 193 of Title 10, Armed Forces.

Section 315(c) of Pub. L. 104-197 provided that: This section [amending this section and section 3303 of this title] shall take effect 30 days after the date of the enactment of this Act [Sept. 16, 1996].

EFFECTIVE DATE OF 1993 AMENDMENT; SAVINGS PROVISION

Amendment by Pub. L. 103-94 effective 120 days after Oct. 6, 1993, but not to release or extinguish any penalty, forfeiture, or liability incurred under amended provision, which is to be treated as remaining in force for purpose of sustaining any proper proceeding or action for enforcement of that penalty, forfeiture, or liability, and no provision of Pub. L. 103-94 to affect any proceedings with respect to which charges were filed on or before 120 days after Oct. 6, 1993, with orders to be issued in such proceedings and appeals taken therefrom as if Pub. L. 103-94 had not been enacted, see section 12 of Pub. L. 103-94, set out as an Effective Date; Savings Provision note under section 7321 of this title.

EFFECTIVE DATE OF 1989 AMENDMENT

Amendment by Pub. L. 101-12 effective 90 days following Apr. 10, 1989, see section 11 of Pub. L. 101-12, set out as a note under section 1201 of this title.

SAVINGS PROVISION

Pub. L. 105-339, § 6(d), Oct. 31, 1998, 112 Stat. 3188, provided that: This section [amending this section and repealing section 1599c of Title 10, Armed Forces] shall be treated as if it had never been enacted for purposes of any personnel action (within the meaning of section 2302 of title 5, United States Code) preceding the date of enactment of this Act [Oct. 31, 1998].

FEDERAL BENEFITS AND NON-DISCRIMINATION

Memorandum of President of the United States, June 17, 2009, 74 F.R. 29393, provided:

Memorandum for the Heads of Executive Departments and Agencies

Millions of hard-working, dedicated, and patriotic public servants are employed by the Federal Government as part of the civilian workforce, and many of these devoted Americans have same-sex domestic partners. Leading companies in the private sector are free to provide to same-sex domestic partners the same benefits they provide to married people of the opposite sex. Executive departments and agencies, however, may only provide benefits on that basis if they have legal authorization to do so. My Administration is not authorized by Federal law to extend a number of available Federal benefits to the same-sex partners of Federal employees. Within existing law, however, my Administration, in consultation with the Secretary of State, who oversees our Foreign Service employees, and the

Director of the Office of Personnel Management, who oversees human resource management for our civil service employees, has identified areas in which statutory authority exists to achieve greater equality for the Federal workforce through extension to same-sex domestic partners of benefits currently available to married people of the opposite sex. Extending available benefits will help the Federal Government compete with the private sector to recruit and retain the best and the brightest employees.

I hereby request the following:

SECTION 1. Extension of Identified Benefits. The Secretary of State and the Director of the Office of Personnel Management shall, in consultation with the Department of Justice, extend the benefits they have respectively identified to qualified same-sex domestic partners of Federal employees where doing so can be achieved and is consistent with Federal law.

SEC. 2. Review of Governmentwide Benefits. The heads of all other executive departments and agencies, in consultation with the Office of Personnel Management, shall conduct a review of the benefits provided by their respective departments and agencies to determine what authority they have to extend such benefits to same-sex domestic partners of Federal employees. The results of this review shall be reported within 90 days to the Director of the Office of Personnel Management, who, in consultation with the Department of Justice, shall recommend to me any additional measures that can be taken, consistent with existing law, to provide benefits to the same-sex domestic partners of Federal Government employees.

SEC. 3. Promoting Compliance with Existing Law Requiring Federal Workplaces to be Free of Discrimination Based on Non-Merit Factors. The Office of Personnel Management shall issue guidance within 90 days to all executive departments and agencies regarding compliance with, and implementation of, the civil service laws, rules, and regulations, including 5 U.S.C. 2302(b)(10), which make it unlawful to discriminate against Federal employees or applicants for Federal employment on the basis of factors not related to job performance.

SEC. 4. General Provisions. (a) Nothing in this memorandum shall be construed to impair or otherwise affect:

(i) Authority granted by law or Executive Order to an agency, or the head thereof; or

(ii) Functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(b) This memorandum shall be implemented consistent with applicable law and subject to the availability of appropriations.

(c) This memorandum is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

SEC. 5. Publication. The Director of the Office of Personnel Management is hereby authorized and directed to publish this memorandum in the Federal Register.

BARACK OBAMA.

EXTENSION OF BENEFITS TO SAME-SEX DOMESTIC PARTNERS OF FEDERAL EMPLOYEES

Memorandum of President of the United States, June 2, 2010, 75 F.R. 32247, provided:

Memorandum for the Heads of Executive Departments and Agencies

For far too long, many of our Government's hard-working, dedicated LGBT employees have been denied equal access to the basic rights and benefits their colleagues enjoy. This kind of systemic inequality undermines the health, well-being, and security not just of our Federal workforce, but also of their families and communities. That is why, last June, I directed the heads of executive departments and agencies (agencies), in consultation with the Office of Personnel Man-

agement (OPM), to conduct a thorough review of the benefits they provide and to identify any that could be extended to LGBT employees and their partners and families. Although legislative action is necessary to provide full equality to LGBT Federal employees, the agencies have identified a number of benefits that can be extended under existing law. OPM, in consultation with the Department of Justice, has provided me with a report recommending that all of the identified benefits be extended.

Accordingly, I hereby direct the following:

SECTION 1. Immediate Actions To Extend Benefits. Agencies should immediately take the following actions, consistent with existing law, in order to extend benefits to the same-sex domestic partners of Federal employees, and, where applicable, to the children of same-sex domestic partners of Federal employees:

(a) The Director of OPM should take appropriate action to:

(i) clarify that the children of employees same-sex domestic partners fall within the definition of child for purposes of Federal child-care subsidies, and, where appropriate, for child-care services;

(ii) clarify that, for purposes of employee assistance programs, same-sex domestic partners and their children qualify as family members ;

(iii) issue a proposed rule that would clarify that employees same-sex domestic partners qualify as family members for purposes of noncompetitive appointments made pursuant to Executive Order 12721 of July 30, 1990;

(iv) issue a proposed rule that would add a Federal retiree's same-sex domestic partner to the list of individuals presumed to have an insurable interest in the employee pursuant to 5 U.S.C. 8339(k)(1), 8420;

(v) clarify that under appropriate circumstances, employees same-sex domestic partners and their children qualify as dependents for purposes of evacuation payments made under 5 U.S.C. 5522 5523; Folio: 1632 [sic]

(vi) amend its guidance on implementing President Clinton's April 11, 1997, memorandum to heads of executive departments and agencies on Expanded Family and Medical Leave Policies to specify that the 24 hours of unpaid leave made available to Federal employees in connection with (i) school and early childhood educational activities; (ii) routine family medical purposes; and (iii) elderly relatives health or care needs, may be used to meet the needs of an employee's same-sex domestic partner or the same-sex domestic partner's children; and

(vii) clarify that employees same-sex domestic partners qualify as dependents for purposes of calculating the extra allowance payable under 5 U.S.C. 5042a to assist employees stationed on Johnston Island, subject to any limitations applicable to spouses.

(b) The Administrator of General Services should take appropriate action to amend the definitions of immediate family and dependent appearing in the Federal Travel Regulations, 41 C.F.R. Chs. 300 304, to include same-sex domestic partners and their children, so that employees and their domestic partners and children can obtain the full benefits available under applicable law, including certain travel, relocation, and subsistence payments.

(c) All agencies offering any of the benefits specified by OPM in implementing guidance under section 3 of this memorandum, including credit union membership, access to fitness facilities, and access to planning and counseling services, should take all appropriate action to provide the same level of benefits that is provided to employees' spouses and their children to employees' same-sex domestic partners and their children.

(d) All agencies with authority to provide benefits to employees outside of the context of title 5, United States Code should take all appropriate actions to ensure that the benefits being provided to employees' spouses and their children are also being provided, at an equivalent level wherever permitted by law, to their employees' same-sex domestic partners and their children.

SEC. 2. Continuing Obligation To Provide New Benefits. In the future, all agencies that provide new benefits to the spouses of Federal employees and their children should, to the extent permitted by law, also provide them to the same-sex domestic partners of their employees and those same-sex domestic partners children. This section applies to appropriated and nonappropriated fund instrumentalities of such agencies.

SEC. 3. Monitoring and Guidance. The Director of OPM shall monitor compliance with this memorandum, and may instruct agencies to provide the Director with reports on the status of their compliance, and prescribe the form Folio: 1633 [sic] and manner of such reports. The Director of OPM shall also issue guidance to ensure consistent and appropriate implementation.

SEC. 4. Reporting. By April 1, 2011, and annually thereafter, the Director of OPM shall provide the President with a report on the progress of the agencies in implementing this memorandum until such time as all recommendations have been appropriately implemented.

SEC. 5. General Provisions. (a) Except as expressly stated herein, nothing in this memorandum shall be construed to impair or otherwise affect:

(i) authority granted by law or Executive Order to an agency, or the head thereof; or
(ii) functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(b) This memorandum shall be implemented consistent with applicable law and subject to the availability of appropriations.

(c) This memorandum is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

SEC. 6. Publication. The Director of OPM is hereby authorized and directed to publish this memorandum in the Federal Register.

BARACK OBAMA.

§ 2303. Prohibited personnel practices in the Federal Bureau of Investigation

(a) Any employee of the Federal Bureau of Investigation who has authority to take, direct others to take, recommend, or approve any personnel action, shall not, with respect to such authority, take or fail to take a personnel action with respect to any employee of the Bureau as a reprisal for a disclosure of information by the employee to the Attorney General (or an employee designated by the Attorney General for such purpose) which the employee or applicant reasonably believes evidences

- (1) a violation of any law, rule, or regulation, or
- (2) mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety.

For the purpose of this subsection, personnel action means any action described in clauses (i) through (x) of section 2302(a)(2)(A) of this title with respect to an employee in, or applicant for, a position in the Bureau (other than a position of a confidential, policy-determining, policymaking, or policy-advocating character).

(b) The Attorney General shall prescribe regulations to ensure that such a personnel action shall not be taken against an employee of the Bureau as a reprisal for any disclosure of information described in subsection (a) of this section.

(c) The President shall provide for the enforcement of this section in a manner consistent with

applicable provisions of sections 1214 and 1221 of this title.

(Added Pub. L. 95-454, title I, § 101(a), Oct. 13, 1978, 92 Stat. 1117; amended Pub. L. 101-12, § 9(a)(1), Apr. 10, 1989, 103 Stat. 34.)

AMENDMENTS

1989 Subsec. (c). Pub. L. 101-12 substituted applicable provisions of sections 1214 and 1221 for the provisions of section 1206.

EFFECTIVE DATE OF 1989 AMENDMENT

Amendment by Pub. L. 101-12 effective 90 days following Apr. 10, 1989, see section 11 of Pub. L. 101-12, set out as a note under section 1201 of this title.

DELEGATION OF RESPONSIBILITIES CONCERNING FBI EMPLOYEES UNDER THE CIVIL SERVICE REFORM ACT OF 1978

Memorandum of President of the United States, Apr. 14, 1997, 62 F.R. 23123, provided:

Memorandum for the Attorney General

By the authority vested in me by the Constitution and laws of the United States of America, including section 301 of title 3, United States Code, I hereby delegate to the Attorney General the functions concerning employees of the Federal Bureau of Investigation vested in the President by section 101(a) of the Civil Service Reform Act of 1978 (Public Law 95-454), as amended by the Whistleblower Protection Act of 1989 (Public Law 101-12), and codified at section 2303(c) of title 5, United States Code, and direct the Attorney General to establish appropriate processes within the Department of Justice to carry out these functions. Not later than March 1 of each year, the Attorney General shall provide a report to the President stating the number of allegations of reprisal received during the preceding calendar year, the disposition of each allegation resolved during the preceding calendar year, and the number of unresolved allegations pending as of the end of the calendar year.

All of the functions vested in the President by section 2303(c) of title 5, United States Code, and delegated to the Attorney General, may be redelegated, as appropriate, provided that such functions may not be redelegated to the Federal Bureau of Investigation.

You are authorized and directed to publish this memorandum in the Federal Register.

WILLIAM J. CLINTON.

§ 2304. Responsibility of the Government Accountability Office

If requested by either House of the Congress (or any committee thereof), or if considered necessary by the Comptroller General, the Government Accountability Office shall conduct audits and reviews to assure compliance with the laws, rules, and regulations governing employment in the executive branch and in the competitive service and to assess the effectiveness and soundness of Federal personnel management.

(Added Pub. L. 95-454, title I, § 101(a), Oct. 13, 1978, 92 Stat. 1118; amended Pub. L. 102-378, § 2(6), Oct. 2, 1992, 106 Stat. 1346; Pub. L. 104-66, title II, § 2181(e), Dec. 21, 1995, 109 Stat. 732; Pub. L. 108-271, § 8(b), July 7, 2004, 118 Stat. 814.)

AMENDMENTS

2004 Pub. L. 108-271 substituted Government Accountability Office for General Accounting Office in section catchline and text.

1995 Pub. L. 104-66 struck out subsec. (a) designation before If requested by and struck out subsec. (b) which read as follows: The General Accounting Office

NATIONAL SECURITY ACT OF 1947

NATIONAL SECURITY ACT OF 1947

[Public Law 235; 61 STAT. 496; July 26, 1947]

AN ACT To promote the national security by providing for a Secretary of Defense; for a National Military Establishment; for a Department of the Army, a Department of the Navy, and a Department of the Air Force; and for the coordination of the activities of the National Military Establishment with other departments and agencies of the Government concerned with the national security.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SHORT TITLE

That this Act may be cited as the “National Security Act of 1947”.

TABLE OF CONTENTS

- SEC. 2. Declaration of Policy.
- SEC. 3. Definitions.

TITLE I—COORDINATION FOR NATIONAL SECURITY

- SEC. 101. National Security Council.
- SEC. 101A. Joint Intelligence Community Council.
- SEC. 102. Director of National Intelligence.
- SEC. 102A. Responsibilities and authorities of the Director of National Intelligence.
- SEC. 103. Office of the Director of National Intelligence.
- SEC. 103A. Deputy Directors of National Intelligence.
- SEC. 103B. National Intelligence Council.
- SEC. 103C. General Counsel.
- SEC. 103D. Civil Liberties Protection Officer.
- SEC. 103E. Director of Science and Technology.
- SEC. 103F. Director of the National Counterintelligence and Security Center.
- SEC. 103G. Chief Information Officer.
- SEC. 103H. Inspector General of the Intelligence Community.
- SEC. 103I. Chief Financial Officer of the Intelligence Community.
- SEC. 103J. Functional Managers for the intelligence community [sic].
- SEC. 104. Central Intelligence Agency.

NATIONAL SECURITY ACT OF 1947

SEC. 104A. Director of the Central Intelligence Agency.

SEC. 104B. Deputy Director of the Central Intelligence Agency.

SEC. 105. Responsibilities of the Secretary of Defense pertaining to the National Intelligence Program.

SEC. 105A. Assistance to United States law enforcement agencies.

SEC. 105B. Disclosure of foreign intelligence acquired in criminal investigations; notice of criminal investigations of foreign intelligence sources.

SEC. 106. Appointment of officials responsible for intelligence-related activities.

SEC. 106A. Director of the National Reconnaissance Office.

SEC. 108. Annual National Security Strategy Report.

SEC. 108A. National intelligence strategy.

SEC. 109. Software licensing.

SEC. 110. National mission of National Geospatial-Intelligence Agency.

SEC. 112. Restrictions on intelligence sharing with the United Nations.

SEC. 113. Detail of intelligence community personnel—intelligence community assignment program.

SEC. 113A. Non-reimbursable detail of other personnel.

SEC. 113B. Special pay authority for science, technology, engineering, or mathematics positions.

SEC. 114. Annual report on hiring and retention of minority employees.

SEC. 115. Limitation on establishment or operation of diplomatic intelligence support centers.

SEC. 116. Travel on any common carrier for certain intelligence collection personnel.

SEC. 117. POW/MIA analytic capability.

SEC. 118. Annual report on financial intelligence on terrorist assets.

SEC. 119. National Counterterrorism Center.

SEC. 119A. National Counter Proliferation Center.

SEC. 119B. National intelligence centers.

SEC. 119C. Foreign Malign Influence Response Center.

SEC. 120. Climate Security Advisory Council.

TITLE II—THE DEPARTMENT OF DEFENSE

SEC. 201. Applicable Laws.

SEC. 205. Department of the Army.

SEC. 206. Department of the Navy.

SEC. 207. Department of the Air Force.

NATIONAL SECURITY ACT OF 1947

TITLE III—MISCELLANEOUS

- SEC. 301. National Security Agency voluntary separation.
- SEC. 302. Authority of Federal Bureau of Investigation to award personal services contracts.
- SEC. 303. Advisory committees and personnel.
- SEC. 304. Reporting of certain employment activities by former intelligence officers and employees.
- SEC. 307. Authorization for appropriations.
- SEC. 308. Definitions.
- SEC. 309. Separability.
- SEC. 310. Effective date.
- SEC. 311. Succession to the Presidency.
- SEC. 312. Repealing and saving provisions.

TITLE V—ACCOUNTABILITY FOR INTELLIGENCE ACTIVITIES

- SEC. 501. General congressional oversight provisions.
- SEC. 502. Reporting of intelligence activities other than covert actions.
- SEC. 503. Presidential approval and reporting of covert actions.
- SEC. 504. Funding of intelligence activities.
- SEC. 505. Notice to Congress of certain transfers of defense articles and defense services.
- SEC. 506. Specificity of National Intelligence Program budget amounts for counterterrorism, counterproliferation, counternarcotics, and counterintelligence.
- SEC. 506A. Budget treatment of costs of acquisition of major systems by the intelligence community.
- SEC. 506B. Annual personnel level assessments for the intelligence community.
- SEC. 506C. Vulnerability assessments of major systems.
- SEC. 506D. Intelligence community business system transformation.
- SEC. 506E. Reports on the acquisition of major systems.
- SEC. 506F. Critical cost growth in major systems.
- SEC. 506G. Future budget projections.
- SEC. 506H. Reports on security clearances.
- SEC. 506I. Summary of intelligence relating to terrorist recidivism of detainees held at United States Naval Station, Guantanamo Bay, Cuba.
- SEC. 507. Dates for submittal of various annual and semiannual reports to the congressional intelligence committees.
- SEC. 508. Certification of compliance with oversight requirements.

NATIONAL SECURITY ACT OF 1947

- SEC. 509. Auditability of certain elements of the intelligence community.
- SEC. 510. Significant interpretations of law concerning intelligence activities.
- SEC. 511. Annual report on violations of law or executive order.
- SEC. 512. Briefings and notifications on counterintelligence activities of the Federal Bureau of Investigation.

TITLE VI—PROTECTION OF CERTAIN NATIONAL SECURITY INFORMATION

- SEC. 601. Protection of identities of certain United States undercover intelligence officers, agents, informants, and sources.
- SEC. 602. Defenses and exceptions.
- SEC. 603. Extraterritorial jurisdiction.
- SEC. 604. Providing information to Congress.
- SEC. 605. Definitions.

TITLE VII—PROTECTION OF OPERATIONAL FILES

- SEC. 701. Operational files of the Central Intelligence Agency.
- SEC. 702. Operational files of the National Geospatial-Intelligence Agency.
- SEC. 703. Operational files of the National Reconnaissance Office.
- SEC. 704. Operational files of the National Security Agency.
- SEC. 705. Operational files of the Defense Intelligence Agency.
- SEC. 706. Protection of certain files of the Office of the Director of National Intelligence.

TITLE VIII—ACCESS TO CLASSIFIED INFORMATION

- SEC. 801. Procedures.
- SEC. 802. Requests by authorized investigative agencies.
- SEC. 803. Security Executive Agent.
- SEC. 804. Exceptions.
- SEC. 805. Definitions.

TITLE IX—APPLICATION OF SANCTIONS LAWS TO INTELLIGENCE ACTIVITIES

- SEC. 901. Stay of sanctions.
- SEC. 902. Extension of stay.
- SEC. 903. Reports.
- SEC. 904. Laws subject to stay.

NATIONAL SECURITY ACT OF 1947

TITLE X—EDUCATION IN SUPPORT OF NATIONAL INTELLIGENCE

SUBTITLE A—SCIENCE AND TECHNOLOGY

- SEC. 1001. Scholarships and work-study for pursuit of graduate degrees in science and technology.
- SEC. 1002. Framework for cross-disciplinary education and training.

SUBTITLE B—FOREIGN LANGUAGES PROGRAM

- SEC. 1011. Program on advancement of foreign languages critical to the intelligence community.
- SEC. 1012. Education partnerships.
- SEC. 1013. Voluntary services.
- SEC. 1014. Regulations.
- SEC. 1015. Definitions.

SUBTITLE C—ADDITIONAL EDUCATION PROVISIONS

- SEC. 1021. Assignment of intelligence community personnel as language students.
- SEC. 1022. Program on recruitment and training.
- SEC. 1023. Educational scholarship program.
- SEC. 1024. Intelligence officer training program.

TITLE XI—OTHER PROVISIONS

- SEC. 1101. Applicability to United States intelligence activities of Federal laws implementing international treaties and agreements.
- SEC. 1102. Counterintelligence initiatives.
- SEC. 1103. Misuse of the Office of the Director of National Intelligence name, initials, or seal.
- SEC. 1104. Prohibited personnel practices in the Intelligence Community.
- SEC. 1105. Semiannual reports on investigations of unauthorized disclosures of classified information.
- SEC. 1106. Inspector General external review panel.
- SEC. 1107. Annual reports on influence operations and campaigns in the United States by the Communist Party of China.
- SEC. 1108. Annual reports on influence operations and campaigns in the United States by the Russian Federation.

NATIONAL SECURITY ACT OF 1947

DECLARATION OF POLICY

SEC. 2. [50 U.S.C. § 3002]

In enacting this legislation, it is the intent of Congress to provide a comprehensive program for the future security of the United States; to provide for the establishment of integrated policies and procedures for the departments, agencies, and functions of the Government relating to the national security; to provide a Department of Defense, including the three military Departments of the Army, the Navy (including naval aviation and the United States Marine Corps), and the Air Force under the direction, authority, and control of the Secretary of Defense; to provide that each military department shall be separately organized under its own Secretary and shall function under the direction, authority, and control of the Secretary of Defense; to provide for their unified direction under civilian control of the Secretary of Defense but not to merge these departments or services; to provide for the establishment of unified or specified combatant commands, and a clear and direct line of command to such commands; to eliminate unnecessary duplication in the Department of Defense, and particularly in the field of research and engineering by vesting its overall direction and control in the Secretary of Defense; to provide more effective, efficient, and economical administration in the Department of Defense; to provide for the unified strategic direction of the combatant forces, or their operation under unified command, and for their integration into an efficient team of land, naval, and air forces but not to establish a single Chief of Staff over the armed forces nor an overall armed forces general staff.

DEFINITIONS

SEC. 3. [50 U.S.C. § 3003]

As used in this Act:

- (1) The term "intelligence" includes foreign intelligence and counterintelligence.
- (2) The term "foreign intelligence" means information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities.
- (3) The term "counterintelligence" means information gathered, and activities conducted, to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities.
- (4) The term "intelligence community" includes the following:
 - (A) The Office of the Director of National Intelligence.
 - (B) The Central Intelligence Agency.
 - (C) The National Security Agency.

NATIONAL SECURITY ACT OF 1947

- (D) The Defense Intelligence Agency.
- (E) The National Geospatial-Intelligence Agency.
- (F) The National Reconnaissance Office.
- (G) Other offices within the Department of Defense for the collection of specialized national intelligence through reconnaissance programs.
- (H) The intelligence elements of the Army, the Navy, the Air Force, the Marine Corps, the Coast Guard, the Federal Bureau of Investigation, the Drug Enforcement Administration, and the Department of Energy.
- (I) The Bureau of Intelligence and Research of the Department of State.
- (J) The Office of Intelligence and Analysis of the Department of the Treasury.
- (K) The Office of Intelligence and Analysis of the Department of Homeland Security.
- (L) Such other elements of any department or agency as may be designated by the President, or designated jointly by the Director of National Intelligence and the head of the department or agency concerned, as an element of the intelligence community.

(5) The terms “national intelligence” and “intelligence related to national security” refer to all intelligence, regardless of the source from which derived and including information gathered within or outside the United States, that—

- (A) pertains, as determined consistent with any guidance issued by the President, to more than one United States Government agency; and
- (B) that involves—
 - (i) threats to the United States, its people, property, or interests;
 - (ii) the development, proliferation, or use of weapons of mass destruction; or
 - (iii) any other matter bearing on United States national or homeland security.

(6) The term “National Intelligence Program” refers to all programs, projects, and activities of the intelligence community, as well as any other programs of the intelligence community designated jointly by the Director of National Intelligence and the head of a United States department or agency or by the President. Such term does not include programs, projects, or activities of the military departments to acquire intelligence solely for the planning and conduct of tactical military operations by United States Armed Forces.

(7) The term “congressional intelligence committees” means—

- (A) the Select Committee on Intelligence of the Senate; and
- (B) the Permanent Select Committee on Intelligence of the House of Representatives.



DEPARTMENT OF DEFENSE

PERSONNEL SECURITY PROGRAM

JANUARY 1987

ADMINISTRATIVE REISSUANCE INCORPORATING
THROUGH CHANGE 3, FEBRUARY 23, 1996

OFFICE OF THE DEPUTY UNDER SECRETARY OF DEFENSE
(POLICY)



OFFICE OF THE UNDER SECRETARY OF DEFENSE

WASHINGTON, D.C. 20301

POLICY

December 16, 1986

FOREWORD

This "Personnel Security Program Regulation" is reissued under the authority of DoD Directive 5200.2, "DoD Personnel Security Program," December 20, 1979. It contains expanded direction and procedures for implementing those references cited in Chapter 1 and in Appendix A of this Regulation that pertain to acceptance and retention of DoD military, civilian, consultant and contractor personnel and of granting such persons access to classified information or assignment to a sensitive position. It also implements such recommendations from the Defense Security Review Commission Report as pertains to personnel security and approved by the Secretary of Defense.

DoD 5200.2-R, "Department of Defense Personnel Security Program," December 1979, is hereby canceled as of December 31, 1986. The effective date of this Regulation is January 1, 1987.

The provisions of this Regulation apply to the Office of the Secretary of Defense (OSD) and activities supported administratively by OSD, the Military Departments, the Organization of the Joint Chiefs of Staff (OJCS), the Unified and Specified Commands, and the Defense Agencies.

This Regulation is mandatory for use by all DoD Components. Heads of DoD Components may issue supplementary instructions when necessary to provide for internal administration of this Regulation within their respective components.

Forward communications, including recommended changes, regarding this Regulation and copies of supplemental instructions issued, through appropriate channels to: Deputy Under Secretary of Defense for Policy, Attention: Director Counter-intelligence and Investigative Programs, Room 3C-267, The Pentagon, Washington, D.C. 20301-2200.

This Regulation is being published in Title 32, Code of Federal Regulations (CFR). DoD Components may obtain copies of this Regulation through their own publications channels. Federal Agencies and the public may obtain copies from the U.S. Department of Commerce, National Technical Information Service, 5285 Port Royal Road, Springfield, VA 22161.



Craig Alderman, Jr.
Deputy

TABLE OF CONTENTS

	<u>Page</u>
FOREWORD	2
TABLE OF CONTENTS	3
REFERENCES	5
DEFINITIONS	8
CHAPTER 1 - GENERAL PROVISIONS	13
C1.1. - PURPOSE AND APPLICABILITY	13
CHAPTER 2 - POLICIES	15
C2.1. - STANDARDS FOR ACCESS TO CLASSIFIED INFORMATION OR ASSIGNMENT TO SENSITIVE DUTIES	15
C2.2. - CRITERIA FOR APPLICATION OF SECURITY STANDARDS	15
C2.3. - TYPES AND SCOPE OF PERSONNEL SECURITY INVESTIGATIONS	18
C2.4. - AUTHORIZED PERSONNEL SECURITY INVESTIGATIVE AGENCIES	22
C2.5. - LIMITATIONS AND RESTRICTIONS	26
CHAPTER 3 - PERSONNEL SECURITY INVESTIGATIVE REQUIREMENTS	29
C3.1. - SENSITIVE POSITIONS	29
C3.2. - CIVILIAN EMPLOYMENT	31
C3.3. - MILITARY APPOINTMENT, ENLISTMENT, AND INDUCTION	33
C3.4. - SECURITY CLEARANCE	34
C3.5. - SPECIAL ACCESS PROGRAMS	46
C3.6. - CERTAIN POSITIONS NOT NECESSARILY REQUIRING ACCESS TO CLASSIFIED INFORMATION	52
C3.7. - REINVESTIGATION	56
C3.8. - AUTHORITY TO WAIVE INVESTIGATIVE REQUIREMENTS	59
CHAPTER 4 - RECIPROCAL ACCEPTANCE OF PRIOR INVESTIGATION AND PERSONNEL SECURITY DETERMINATIONS	60
CHAPTER 5 - REQUESTING PERSONNEL SECURITY INVESTIGATIONS	63
CHAPTER 6 - ADJUDICATION	66
CHAPTER 7 - ISSUING CLEARANCE AND GRANTING ACCESS	70
CHAPTER 8 - UNFAVORABLE ADMINISTRATIVE ACTIONS	73
C8.1. - REQUIREMENTS	73
C8.2. - PROCEDURES	76
C8.3. - REINSTATEMENT OF CIVILIAN EMPLOYEES	78

CHAPTER 9 - CONTINUING SECURITY	80
C9.1. - EVALUATING CONTINUED SECURITY ELEGIBILITY	80
C9.2. - SECURITY EDUCATION	82
CHAPTER 10 - SAFEGUARDING PERSONNEL SECURITY INVESTIGATIVE RECORDS	86
CHAPTER 11- PROGRAM MANAGEMENT	89
CHAPTER 12 - DEFENSE CLEARANCE AND INVESTIGATIONS INDEX (DCII)	92
APPENDICES	
APPENDIX 1 - INVESTIGATIVE SCOPE	97
APPENDIX 2 - REQUEST PROCEDURES	111
APPENDIX 3 - TABLES FOR REQUESTING INVESTIGATIONS	117
APPENDIX 4 - REPORTING OF NONDEROGATORY CASES	124
APPENDIX 5 - DOD SECURITY CLEARANCE AND/OR SCI ACCESS DETERMINATION AUTHORITIES	125
APPENDIX 6 - GUIDELINES FOR CONDUCTING PRE-NOMINATION PERSONAL INTERVIEWS	129
APPENDIX 7 - (LEFT BLANK FOR FUTURE USE)	131
APPENDIX 8 - ADJUDICATIVE GUIDELINES FOR DETERMINING ELIGIBILITY FOR ACCESS TO CLASSIFIED INFORMATION	132
APPENDIX 9 - OVERSEAS INVESTIGATIONS	153
APPENDIX 10 - ADP POSITION CATEGORIES AND CRITERIA FOR DESIGNATING POSITIONS	162
APPENDIX 11 - SAMPLE NOTIFICATIONS FOR ADVERSE PERSONNEL SECURITY DETERMINATIONS	164
APPENDIX 12 - STRUCTURE AND FUNCTIONING OF THE PERSONNEL SECURITY APPEAL BOARD	183
APPENDIX 13 - CONDUCT OF APERSONAL APPEARANCE BEFORE AN ADMINISTRATIVE JUDGE (AJ)	185

REFERENCES

- (a) DoD 5200.2-R, "DoD Personnel Security Program," January 1987, authorized by [DoD Directive 5200.2, May 6, 1992](#)
- (b) DoD 5220.22-R, "Industrial Security Regulation," authorized by [DoD Directive 5220.22](#), December 8, 1980
- (c) [DoD Directive 5220.6](#), "Defense Industrial Personnel Security Clearance Review Program," [February 2, 1992](#)
- (d) Reference Not Used
- (e) [Public Law 88-290, "National Security Agency - Personnel Security Procedures," March 26, 1964 \(78 STAT. 168\)](#)
- (f) [Public Law 86-36, "National Security Agency Officers and Employees," May 29, 1959 \(73 Stat. 63\)](#)
- (g) Executive Order 10450, "Security Requirements for Government Employment," April 27, 1953
- (h) Executive Order 12333, "United States Intelligence Activities," December 4, 1981
- (i) [DoD Directive 5210.45](#), "Personnel Security in the National Security Agency," May 9, 1964
- (j) [Executive Order 1295.8, "Classified National Security Information," April 17, 1995](#)
- (k) Executive Order 11935, "Citizenship Requirements for Federal Employment," September 2, 1976
- (l) Director of Central Intelligence Directive (DCID) No. 1/14, "Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information (SCI)," January 22, 1992
- (m) [Section 552a of title 5, United States Code](#)
- (n) [DoD Directive 5100.23](#), "Administrative Arrangements for the National Security Agency, May 17, 1967
- (o) Agreement Governing the Conduct of Defense Department Counterintelligence Activities in Conjunction with the Federal Bureau of Investigation, April 5, 1979
- (p) [DoD Directive 5210.48](#), "DoD Polygraph Program," December 24, 1984
- (q) DoD 5200.1-R, "Information Security Program Regulation," June 1986, authorized by [DoD Directive 5200.1, "DoD Information Security Program," June 7, 1982](#)
- (r) [DoD Directive 5210.55](#), "Selection of DoD Military and Civilian Personnel and Contractor Employees for Assignment to Presidential Support Activities," July 6, 1977
- (s) [DoD Directive 5210.42, "Nuclear Weapon Personnel Reliability Program \(PRP\)," May 25, 1993](#)

- (t) DoD Directive 5200.8, "Security of Military Installations and Resources," April 25, 1991
- (u) DoD 1401.1-M, "Personnel Policy Manual for Nonappropriated Fund Instrumentalities," January 1981, authorized by DoD Instruction 1401.1, November 15, 1985
- (v) DoD 5030.49-R, "Customs Inspection," May 1977, authorized by DoD Directive 5030.49, January 6, 1984
- (w) DoD Instruction 5210.25, "Assignment of American National Red Cross and United Service Organizations, Inc., Employees to Duty with the Military Services," May 12, 1983
- (x) DoD Directive 5210.46, "DoD Building Security for the National Capital Region," January 28, 1982
- (y) DoD Directive 5210.65, "Chemical Agent Security Program," October 15, 1986
- (z) DoD Directive 5210.2, "Access to and Dissemination of Restricted Data," January 12, 1978
 - (aa) DoD Directive 5400.7, "DoD Freedom of Information Act Program," May 13, 1988
 - (bb) DoD Directive 5400.11, "Department of Defense Privacy Program," June 9, 1982
 - (cc) 5 CFR, Part 732, "National Security Positions," January 1, 1995
 - (dd) Section 3571 of title 5, United States Code
 - (ee) Section 3 of Public Law 89-380, "Back Pay Act of 1966," March 30, 1966 (80 Stat. 94)
- (ff) Executive Order 9835, "Prescribing Procedures for the Administration of an Employee Loyalty Program in the Executive Branch of the Government," issued 1947 (superseded by Executive Order 10450)
- (gg) Public Law 83-703, "Atomic Energy Act of 1954," as amended, August 30, 1954
- (hh) DoD Directive 5105.42, "Defense Investigative Service," June 14, 1985
- (ii) Defense Investigative Service 20-1-M, "Manual for Personnel Security Investigations," January 1993
- (jj) Memorandum of Understanding between the Director, White House Military Office and the Special Assistant to the Secretary and Deputy Secretary of Defense, "White House Clearances," July 30, 1980
- (kk) USSAN Instruction 1-69, April 21, 1982 (Enclosure 2 to DoD Directive 5100.55, "United States Security Authority for North Atlantic Treaty Organization Affairs," April 21, 1982)
- (ll) DoD Directive 5230.11, "Disclosure of Classified Military Information to Foreign Governments and International Organizations," June 16, 1982
- (mm) DoD Directive 5100.3, "Support of the Headquarters of Unified, Specified, and Subordinate Joint Commands," November 1, 1988
- (nn) Public Law 96-456, "Classified Information Procedures Act," October 15, 1980 (94 Stat. 2025)

- (oo) DoD Directive 5142.1, "Assistant Secretary of Defense (Legislative Affairs)," July 2, 1982
- |(pp) Section 7532 of title 5, United States Code
- |(qq) DoD Directive O-5205.7, "Special Access Program (SAP) Policy," January 4, 1989
- |(rr) National Security Directive 63, "Single Scope Background Investigations," October 21, 1991

DL1. DEFINITIONS

DL1.1.1. Access. The ability and opportunity to obtain knowledge of classified information. An individual, in fact, may have access to classified information by being in a place where such information is kept, if the security measures that are in force do not prevent him from gaining knowledge of such information.

DL1.1.2. Adverse Action. A removal from employment, suspension from employment of more than 14 days, reduction in grade, reduction in pay, or furlough of 30 days or less.

DL1.1.3. Background Investigation (BI). A personnel security investigation consisting of both record reviews and interviews with sources of information as prescribed in paragraph AP1.1.1.3., Appendix 1, this Regulation, covering the most recent 5 years of an individual's life or since the 18th birthday, whichever is shorter, provided that at least the last 2 years are covered and that no investigation will be conducted prior to an individual's 16th birthday.

DL1.1.4. Classified Information. Official information or material that requires protection in the interests of national security and that is classified for such purpose by appropriate classifying authority in accordance with the provisions of Executive Order 12356 (reference (j)).

DL1.1.5. Defense Central Security Index (DCSI). An automated sub-system of the Defense Central Index of Investigations (DCII) designed to record the issuance, denial or revocation of security clearances, access to classified information, or assignment to a sensitive position by all DoD Components for military, civilian, and contractor personnel. The DCSI will serve as the central DoD repository of security related actions in order to assist DoD security officials in making sound clearance and access determinations. The DCSI shall also serve to provide accurate and reliable statistical data for senior DoD officials, Congressional committees, the General Accounting Office and other authorized Federal requesters.

DL1.1.6. DoD Component. Includes the Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, The DoD Field Activities, and all other organizational entities within the Department of Defense (hereafter referred to collectively as "the DoD Components").

DL1.1.7. Entrance National Agency Check (ENTNAC). A personnel security

investigation scoped and conducted in the same manner as a National Agency Check (NAC) except that a technical fingerprint search of the files of the Federal Bureau of Investigation is not conducted.

DL1.1.8. Head of DoD Component. The Secretary of Defense; the Secretaries of the Military Departments; the Chairman, Joint Chiefs of Staff; and the Commanders of the Combatant Commands; and the Directors of Defense Agencies.

DL1.1.9. Immigrant Alien. Any alien lawfully admitted into the United States under an immigration visa for permanent residence.

DL1.1.10. Interim Security Clearance. A security clearance based on the completion of minimum investigative requirements, which is granted on a temporary basis, pending the completion of the full investigative requirements.

DL1.1.11. Limited Access Authorization. Authorization for access to Confidential or Secret information granted to non-United States citizens and immigrant aliens, which is limited to only that information necessary to the successful accomplishment of their assigned duties and based on a background investigation scoped for 10 years (paragraph AP1.1.1.3., Appendix 1).

DL1.1.12. Minor Derogatory Information. Information that, by itself, is not of sufficient importance or magnitude to justify an unfavorable administrative action in a personnel security determination.

DL1.1.13. National Agency Check (NAC). A personnel security investigation consisting of a records review of certain national agencies as prescribed in paragraph AP1.1.1.1., Appendix 1, this Regulation, including a technical fingerprint search of the files of the Federal Bureau of Investigation (FBI).

DL1.1.14. National Agency Check Plus Written Inquiries (NACI). A personnel security investigation conducted by the Office of Personnel Management, combining a NAC and written inquiries to law enforcement agencies, former employers and supervisors, references and schools.

DL1.1.15. DoD National Agency Check Plus Written Inquiries (DNACI). A personnel security investigation conducted by the Defense Investigative Service (DIS) for access to SECRET information consisting of a NAC, credit bureau check, and written inquiries to current and former employers (see paragraph AP1.1.1.2., Appendix 1), covering a 5-year scope.

DL1.1.16. National Security. National security means the national defense and foreign relations of the United States.

DL1.1.17. Need-to-Know A determination made by a possessor of classified information that a prospective recipient, in the interest of national security, has a requirement for access to, knowledge, or possession of the classified information in order to perform tasks or services essential to the fulfillment of an official United States Government program. Knowledge, possession of, or access to, classified information shall not be afforded to any individual solely by virtue of the individual's office, position, or security clearance.

DL1.1.18. Periodic Reinvestigation (PR). An investigation conducted every 5 years for the purpose of updating a previously completed background or special background investigation on persons occupying positions referred to in paragraphs C3.7. through C3.7.10. The scope will consist of a personal interview, NAC, LACs, credit bureau checks, employment records, employment references and developed character references and will normally not exceed the most recent 5-year period.

DL1.1.19. Personnel Security Investigation (PSI). Any investigation required for the purpose of determining the eligibility of DoD military and civilian personnel, contractor employees, consultants, and other persons affiliated with the Department of Defense, for access to classified information, acceptance or retention in the Armed Forces, assignment or retention in sensitive duties, or other designated duties requiring such investigation. PSIs include investigations of affiliations with subversive organizations, suitability information, or hostage situations (see paragraph C2.4.3.) conducted for the purpose of making personnel security determinations. They also include investigations of allegations that arise subsequent to adjudicative action and require resolution to determine an individual's current eligibility for access to classified information or assignment or retention in a sensitive position.

DL1.1.20. Scope The time period to be covered and the sources of information to be contacted during the prescribed course of a PSI.

DL1.1.21. Security Clearance. A determination that a person is eligible under the

standards of this Regulation for access to classified information.

DL1.1.22. Senior Officer of the Intelligence Community (SOIC). The DoD Senior Officers of the Intelligence Community include: the Director, National Security Agency/Central Security Service; Director, Defense Intelligence Agency; Assistant Chief of Staff for Intelligence, U.S. Army; Assistant Chief of Staff for Intelligence, U.S. Air Force; and the Director of Naval Intelligence, U.S. Navy.

DL1.1.23. Sensitive Position. Any position so designated within the Department of Defense, the occupant of which could bring about, by virtue of the nature of the position, a materially adverse effect on the national security. All civilian positions are either critical-sensitive, noncritical-sensitive, or nonsensitive as described in paragraph C3.1.1.

DL1.1.24. Significant Derogatory Information. Information that could, in itself, justify an unfavorable administrative action, or prompt an adjudicator to seek additional investigation or clarification.

DL1.1.25. Special Access Program. Any program imposing "need-to-know" or access controls beyond those normally provided for access to Confidential, Secret, or Top Secret information. Such a program may include, but not be limited to, special clearance, adjudication, investigative requirements, material dissemination restrictions, or special lists of persons determined to have a need-to-know.

DL1.1.26. Special Background Investigation (SBI). A personnel security investigation consisting of all of the components of a BI plus certain additional investigative requirements as prescribed in paragraph AP1.1.1.4., Appendix 1, this Regulation. The period of investigation for an SBI is the last 15 years or since the 18th birthday, whichever is shorter, provided that the last 2 full years are covered and that no investigation will be conducted prior to an individual's 16th birthday.

DL1.1.27. Special Investigative Inquiry (SII). A supplemental personnel security investigation of limited scope conducted to prove or disprove relevant allegations that have arisen concerning a person and who, at the time of the allegation, holds a security clearance or otherwise occupies a position that requires a personnel security determination under the provision of this Regulation.

DL1.1.28. Service. Honorable active duty (including attendance at the military academies), membership in ROTC Scholarship Program, Army and Air Force National Guard, Military Reserve Force (including active status and ready reserve), civilian employment in Government service, or civilian employment with a DoD contractor or as a consultant involving access under the DoD Industrial Security Program. Continuity of service is maintained with change from one status to another as long as there is no single break in service greater than 12 months.

DL1.1.29. Unfavorable Administrative Action. Adverse action taken as the result of personnel security determinations and unfavorable personnel security determinations as defined in this Regulation.

DL1.1.30. Unfavorable Personnel Security Determination. A denial or revocation of clearance for access to classified information; denial or revocation of access to classified information; denial or revocation of a Special Access authorization (including access to SCI); nonappointment to or nonselection for appointment to a sensitive position; nonappointment to or nonselection for any other position requiring a trustworthiness determination under this Regulation; reassignment to a position of lesser sensitivity or to a nonsensitive position; and nonacceptance for or discharge from the Armed Forces when any of the foregoing actions are based on derogatory information of personnel security significance.

DL1.1.31. United States Citizen. (Native Born) - A person born in one of the 50 United States, Puerto Rico, Guam, American Samoa, Northern Mariana Islands, U.S. Virgin Islands; or the Republic of Panama (former Panama Canal Zone) (if the father or mother (or both) was or is, a citizen of the United States).

C1. CHAPTER 1

DEPARTMENT OF DEFENSE PERSONNEL SECURITY PROGRAM GENERAL PROVISIONS

C1.1. PURPOSE AND APPLICABILITY

C1.1. Purpose

C1.1.1. To establish policies and procedures to ensure that acceptance and retention of personnel in the Armed Forces, acceptance and retention of civilian employees in the Department of Defense, and granting members of the Armed Forces, DoD civilian employees, DoD contractors, and other affiliated persons access to classified information are clearly consistent with the interests of national security.

C1.1.2. This Regulation:

C1.1.2.1. Establishes DoD personnel security policies and procedures;

C1.1.2.2. Sets forth the standards, criteria, and guidelines upon which personnel security determinations shall be based;

C1.1.2.3. Prescribes the kinds and scopes of personnel security investigations required;

C1.1.2.4. Details the evaluation and adverse action procedures by which personnel security determinations shall be made; and

C1.1.2.5. Assigns overall program management responsibilities.

C1.2. Applicability

C1.2.1. This Regulation implements the Department of Defense Personnel Security Program and takes precedence over all other departmental issuances affecting that program.

C1.2.2. All provisions of this Regulation apply to DoD civilian personnel, members of the Armed Forces, excluding the Coast Guard in peacetime, contractor personnel and other personnel who are affiliated with the Department of Defense except that the unfavorable administrative action procedures pertaining to contractor personnel requiring access to classified information are contained in DoD 5220.22-R

(reference (b)) and in DoD Directive 5220.6 (reference (c)).

C1.2.3. The policies and procedures THAT govern the National Security Agency are prescribed by Public Laws 88-290 and 86-36, Executive Orders 10450 and 12333, DoD Directive 5210.45, Director of Central Intelligence Directive (DCID) 1/14 (references (e), (f), (g), (h), (i), and (l) respectively), and regulations of the National Security Agency.

C1.2.4. Under combat conditions or other military exigencies, an authority in paragraph AP6.1., Appendix 6, may waive such-provisions of this regulation as the circumstances warrant.

C2. CHAPTER 2

POLICIES

C2.1. STANDARDS FOR ACCESS TO CLASSIFIED INFORMATION OR ASSIGNMENT TO SENSITIVE DUTIES

C2.1.1. General. Only United States citizens shall be granted a personnel security clearance, assigned to sensitive duties, or granted access to classified information unless an authority designated in Appendix 6 has determined that, based on all available information, there are compelling reasons in furtherance of the Department of Defense mission, including, special expertise, to assign an individual who is not a citizen to sensitive duties or grant a Limited Access Authorization to classified information. Non-U.S. citizens may be employed in the competitive service in sensitive civilian positions only when specifically approved by the Office of Personnel Management, pursuant to E.O. 11935 (reference (k)). Exceptions to these requirements shall be permitted only for compelling national security reasons.

C2.1.2. Clearance and Sensitive Position Standard. The personnel security standard that must be applied to determine whether a person is eligible for access to classified information or assignment to sensitive duties is whether, based on all available information, the person's loyalty, reliability, and trustworthiness are such that entrusting the person with classified information or assigning the person to sensitive duties is clearly consistent with the interests of national security.

C2.1.3. Military Service Standard. The personnel security standard that must be applied in determining whether a person is suitable under national security criteria for appointment, enlistment, induction, or retention in the Armed Forces is that, based on all available information, there is no reasonable basis for doubting the person's loyalty to the Government of the United States.

C2.2. CRITERIA FOR APPLICATION OF SECURITY STANDARDS

C2.2.1. Criteria for Application of Security Standards. The ultimate decision in applying either of the security standards set forth in paragraph C2.1.2. and C2.1.3., above, must be an overall common sense determination based upon all available facts. The criteria for determining eligibility for a clearance under the security standard shall include, but not be limited to the following:

C2.2.1.1. Commission of any act of sabotage, espionage, treason, terrorism,

anarchy, sedition, or attempts thereat or preparation therefor, or conspiring with or aiding or abetting another to commit or attempt to commit any such act.

C2.2.1.2. Establishing or continuing a sympathetic association with a saboteur, spy, traitor, seditionist, anarchist, terrorist, revolutionist, or with an espionage or other secret agent or similar representative of a foreign nation whose interests may be inimical to the interests of the United States, or with any person who advocates the use of force or violence to overthrow the Government of the United States or to alter the form of Government of the United States by unconstitutional means.

C2.2.1.3. Advocacy or use of force or violence to overthrow the Government of the United States or to alter the form of Government of the United States by unconstitutional means.

C2.2.1.4. Knowing membership with the specific intent of furthering the aims of, or adherence to and active participation in any foreign or domestic organization, association, movement, group or combination of persons (hereafter referred to as organizations), which unlawfully advocates or practices the commission of acts of force or violence to prevent others from exercising their rights under the Constitution or laws of the United States or of any State or which seeks to overthrow the Government of the United States or any State or subdivision thereof by unlawful means.

C2.2.1.5. Unauthorized disclosure to any person of classified information, or of other information, disclosure of which is prohibited by Statute, Executive Order or Regulation.

C2.2.1.6. Performing or attempting to perform one's duties, acceptance and active maintenance of dual citizenship, or other acts conducted in a manner which serve or which could be expected to serve the interests of another government in reference to the interests of the United States.

C2.2.1.7. Disregard of public law, Statutes, Executive Orders or Regulations including violation of security regulations or practices.

C2.2.1.8. Criminal or dishonest conduct.

C2.2.1.9. Acts of omission or commission that indicate poor judgment, unreliability or untrustworthiness.

C2.2.1.10. Any behavior or illness, including any mental condition, which, in the opinion of competent medical authority, may cause a defect in judgment or reliability with due regard to the transient or continuing effect of the illness and the medical findings in such case.

C2.2.1.11. Vulnerability to coercion, influence, or pressure that may cause conduct contrary to the national interest. This may be:

C2.2.1.11.1. The presence of immediate family members or other persons to whom the applicant is bonded by affection or obligation in a nation (or areas under its domination) whose interests may be inimical to those of the United States; or

C2.2.1.11.2. Any other circumstances that could cause the applicant to be vulnerable.

C2.2.1.12. Excessive indebtedness, recurring financial difficulties, or unexplained affluence.

C2.2.1.13. Habitual or episodic use of intoxicants to excess.

C2.2.1.14. Illegal or improper use, possession, transfer, sale or addiction to any controlled or psychoactive substance, narcotic, cannabis or other dangerous drug.

C2.2.1.15. Any knowing and willful falsification, cover up, concealment, misrepresentation, or omission of a material fact from any written or oral statement, document, form or other representation or device used by the Department of Defense or any other Federal Agency.

C2.2.1.16. Failing or refusing to answer or-to-authorize others to answer questions or provide information required by a congressional committee, court, or agency in the course of an official inquiry whenever such answers or information concern relevant and material matters pertinent to an evaluation of the individual's trustworthiness, reliability, and judgment.

C2.2.1.17. Acts of sexual misconduct or perversion indicative of moral turpitude, poor judgment, or lack of regard for the laws of society.

C2.3. TYPES AND SCOPE OF PERSONNEL SECURITY INVESTIGATIONS

C2.3.1. General. The types of personnel security investigations authorized below vary in scope of investigative effort required to meet the purpose of the particular investigation. No other types are authorized. The scope of a PSI may be neither raised nor lowered without the approval of the Deputy Under Secretary of Defense for Policy.

C2.3.2. National Agency Check (NAC) Essentially, a NAC is a records check of designated agencies of the Federal Government that maintain record systems containing information relevant to making a personnel security determination. An ENTNAC is a NAC (scope as outlined in paragraph AP1.1.1., Appendix 1) conducted on inductees and first-term enlistees, but lacking a technical fingerprint search. ANAC is also an integral part of each BI, SBI, and Periodic Reinvestigation (PR). Chapter 3 prescribes when a NAC is required.

C2.3.3. National Agency Check plus Written Inquiries. The Office of Personnel Management (OPM) conducts a NAC plus Written Inquiries (NACIs) on civilian employees for all Departments and Agencies of the Federal Government, pursuant to E.O. 10450 (reference (g)). NACIs are considered to meet the investigative requirements of this Regulation for a nonsensitive or noncritical sensitive position and/or up to a SECRET clearance and, in addition to the NAC, include coverage of law enforcement agencies, former employers and supervisors, references, and schools covering the last 5 years.

C2.3.4. DoD National Agency Check (DNCI) Plus Written Inquiries. DIS will conduct a DNACI, consisting of the scope contained in paragraph AP1.1.1.2., Appendix 1, for DoD military and contractor personnel for access to SECRET information. Chapter 3 prescribes when a DNACI is required.

C2.3.5. Background Investigation (BI). The BI is the principal type of investigation conducted when an individual requires TOP SECRET clearance or is to be assigned to a critical sensitive position. The BI normally covers a 5-year period and consists of a subject interview, NAC, LACs, credit checks, developed character references (3), employment records checks, employment references (3), and select scoping as required to resolve unfavorable or questionable information. (See paragraph AP1.1.1.3., Appendix 1). Chapter 3 prescribes when a BI is required.

C2.3.6. Special Background Investigation (SBI)

C2.3.6.1. An SBI is essentially a BI providing additional coverage both in

period of time as well as sources of information, scoped in accordance with the provisions of DCID 1/14 (reference (1)) but without the personal interview. While the kind of coverage provided for by the SBI determines eligibility for access to SCI, the Department of Defense has adopted this coverage for certain other Special Access programs. Chapter 3 prescribes when an SBI is required.

C2.3.6.2. The OPM, FBI, Central Intelligence Agency (CIA), Secret Service, and the Department of State conduct specially scoped BIs under the provisions of DCID 1/14. Any investigation conducted by one of the above-cited Agencies under DCID 1/14 standards is considered to meet the SBI investigative requirements of this Regulation.

C2.3.6.3. The detailed scope of an SBI is set forth in paragraph AP1.1.1.4., Appendix 1.

C2.3.7. Special Investigative Inquiry (SII)

C2.3.7.1. A Special Investigative Inquiry is a personnel security investigation conducted to prove or disprove allegations relating to the criteria outlined in paragraph C2.2.1. of this Regulation, except current criminal activities (see paragraph C2.4.3.4.), that have arisen concerning an individual upon whom a personnel security determination has been previously made and who, at the time of the allegation, holds a security clearance or otherwise occupies a position that requires a trustworthiness determination.

C2.3.7.2. Special Investigative Inquiries are scoped as necessary to address the specific matters requiring resolution in the case concerned and generally consist of record checks and/or interviews with potentially knowledgeable persons. An SII may include an interview with the subject of the investigation when necessary to resolve conflicting information and/or to provide an opportunity to refute or mitigate adverse information.

C2.3.7.3. In those cases when there is a disagreement between Defense Investigative Service (DIS) and the requester as to the appropriate scope of the investigation, the matter may be referred to the Deputy Under Secretary of Defense for Policy for resolution.

C2.3.8. Periodic Reinvestigation (PR). As referred to in paragraph C3.7.1. and other national directives, certain categories of duties, clearance, and access require the conduct of a PR every five years according to the scope outlined in paragraph AP1.1.1.5., Appendix 1. The PR scope applies to military, civilian, contractor, and foreign national personnel.

C2.3.9. Personal Interview. Investigative experience over the years has demonstrated that, given normal circumstances, the subject of a personnel security investigation is the best source of accurate and relevant information concerning the matters under consideration. Further, restrictions imposed by the Privacy Act of 1974 (reference (m)) dictate that Federal investigative agencies collect information to the greatest extent practicable directly from the subject when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs. Accordingly, personal interviews are an integral part of the DoD personnel security program and shall be conducted in accordance with the requirements set forth in the following paragraphs of this section.

C2.3.9.1. BI/PR. A personal interview shall be conducted by a trained DIS agent as part of each BI and PR.

C2.3.9.2. Resolving Adverse Information. A personal interview of the subject shall be conducted by a DIS agent (or, when authorized, by investigative personnel of other DoD investigative organizations designated in this Regulation to conduct personnel security investigations), when necessary, as part of each Special Investigative Inquiry, as well as during the course of initial or expanded investigations, to resolve or clarify any information which may impugn the subject's moral character, threaten the subject's future federal employment, raise the question of subject's security clearability, or be otherwise stigmatizing.

C2.3.9.3. Hostage Situation. A personal interview shall be conducted by a DIS agent (or, when authorized, by investigative personnel of other DoD investigative organizations designated in this Regulation to conduct personnel security investigations) in those instances in which an individual has immediate family members or other persons bound by ties of affection or obligation who reside in a nation whose interests are inimical to the interests of the United States. (See paragraph C2.4.4.)

C2.3.9.4. Applicants/Potential Nominees for DoD Military or Civilian Positions Requiring Access to SCI or Other Positions Requiring SBI. A personal interview of the individual concerned shall be conducted, to the extent feasible, as part of the selection process for applicants/potential nominees for positions requiring access to SCI or completion of an SBI. The interview shall be conducted by a designee of the Component to which the applicant or potential nominee is assigned. Clerical personnel are not authorized to conduct these interviews. Such interviews shall be conducted utilizing resources in the order of priority indicated below:

C2.3.9.4.1. Existing personnel security screening systems (e.g., Air Force

Assessment Screening Program, Naval Security Group Personnel Security Interview Program, U.S. Army Personnel Security Screening Program); or

C2.3.9.4.2. Commander of the nominating organization or such official as he or she has designated in writing (e.g., Deputy Commander, Executive Officer, Security Officer, Security Manager, S-2, Counterintelligence Specialist, Personnel Security Specialist, or Personnel Officer); or

C2.3.9.4.3. Agents of investigative agencies in direct support of the DoD Component concerned.

C2.3.9.5. Administrative Procedures

C2.3.9.5.1. The personal interview required by paragraph C2.3.9.4., above, shall be conducted in accordance with Appendix 6.

C2.3.9.5.2. For those investigations requested subsequent to the personal interview requirements of paragraph C2.3.9.4., above, the following procedures apply:

C2.3.9.5.2.1. The DD Form 1879 (Request for Personnel Security Investigation) shall be annotated under Item 20 (Remarks) with the statement, "Personal Interview Conducted by (cite the duty assignment of the designated official (e.g., Commander, Security Officer, Personnel Security Specialist, etc.))" in all cases in which an SBI is subsequently requested.

C2.3.9.5.2.2. Unfavorable information developed through the personal interview required by paragraph C2.3.9.4., above, will be detailed in a written report attached to the DD Form 1879 to include full identification of the interviewer. Failure to provide such information may result in conduct of an incomplete investigation by DIS.

C2.3.9.5.2.3. Whenever it is determined that it is not feasible to conduct the personal interview required by paragraph C2.3.9.4., above, prior to requesting the SBI, the DD Form 1879 shall be annotated under Item 20 citing the reason for not conducting the interview.

C2.3.10. Expanded Investigation. If adverse or questionable information relevant to a security determination is developed during the conduct of a personnel security investigation, regardless of type, the investigation shall be expanded, consistent with the restrictions in paragraph C2.5.5., to the extent necessary to substantiate or disprove the adverse or questionable information.

C3.2.3. Noncritical-Sensitive Positions

C3.2.3.1. An NACI shall be requested and the NAC portion favorably completed before a person is appointed to a noncritical-sensitive position (for exceptions see paragraph C3.2.5.). An ENTNAC, NAC or DNACI conducted during military or contractor employment may also be used for appointment provided a NACI has been requested from OPM and there is no more than 12 months break in service since completion of the investigation.

C3.2.3.2. Seasonal employees (including summer hires) normally do not require access to classified information. For those requiring access to classified information the appropriate investigation is required. The request for the NAC (or NACI) should be submitted to DIS by entering "SH"(summer hire) in red letters approximately one inch high on the DD Form 398-2, "Personnel Security Questionnaire (National Agency Checklist)." Additionally, to ensure expedited processing by DIS, summer hire requests should be assembled and forwarded to DIS in bundles, when appropriate.

C3.2.4. Critical-Sensitive Positions. A BI shall be favorably completed prior to appointment to critical-sensitive positions (for exceptions see paragraph C3.2.5.). Certain critical-sensitive positions require a preappointment SBI in accordance with section C3.5. of this chapter. Preappointment BIs and SBIs will be conducted by DIS.

C3.2.5. Exceptions

C3.2.5.1. Noncritical-sensitive. In an emergency, a noncritical-sensitive position may be occupied pending the completion of the NACI if the head of the requesting organization finds that the delay in appointment would be harmful to the national security and such finding is reduced to writing and made part of the record. In such instances, the position may be filled only after the NACI has been requested.

C3.2.5.2. Critical-sensitive. In an emergency, a critical-sensitive position may be occupied pending completion of the BI (or SBI, as appropriate) if the head of the requesting organization finds that the delay in appointment would be harmful to the national security and such finding is reduced to writing and made a part of the record. In such instances, the position may be filled only when the NAC portion of the BI (or SBI) or a previous valid NACI, NAC or ENTNAC has been completed and favorably adjudicated.

C3.2.6. Mobilization of DoD Civilian Retirees. The requirements contained in paragraph C3.2.1. of this section, regarding the type of investigation required by position sensitivity for DoD civilian retirees temporary appointment when the break in employment is greater than 12 months, should either be expedited or waived for the purposes of mobilizing selected reemployed annuitants under the provisions of Title 5, United States Code, depending upon the degree of sensitivity of the position to which assigned. Particular priority should be afforded to newly assigned personnel assigned to the defense intelligence and security agencies with respect to granting security clearances in an expeditious manner under paragraph C3.2.1. of this section.

C3.3. MILITARY APPOINTMENT, ENLISTMENT, AND INDUCTION

C3.3.1. General. The appointment, enlistment, and induction of each member of the Armed Forces or their Reserve components shall be subject to the favorable completion of a personnel security investigation. The types of investigation required are set forth in this section.

C3.3.2. Entrance Investigation

C3.3.2.1. An ENTNAC shall be conducted on each enlisted member of the Armed Forces at the time of initial entry into the service. A DNACI shall be conducted on each commissioned officer, except as permitted by paragraph C3.3.4. of this section, warrant officer, cadet, midshipman, and Reserve Officers Training Candidate, at the time of appointment. A full NAC shall be conducted upon reentry of any of the above when there has been a break in service greater than 12 months.

C3.3.2.2. If an officer or warrant officer candidate has been the subject of a favorable NAC or ENTNAC and there has not been a break in service of more than 12 months, a new NAC is not authorized. This includes ROTC graduates who delay entry onto active duty pending completion of their studies.

C3.3.2.3. All derogatory information revealed during the enlistment or appointment process that results in a moral waiver will be fully explained on a written summary attached to the DD Form 398-2.

C3.3.3. Reserve Components and National Guard. Reserve component and National Guard personnel not on active duty are subject to the investigative requirements of this chapter.

C3.3.4. Exceptions for Certain Commissioned Officers of Reserve Components.

The requirements for entrance investigation shall be rigidly adhered to except as follows. Healthcare professionals, chaplains, and attorneys may be commissioned in the Reserve components prior to completion of a DNACI provided that:

C3.3.4.1. A DNACI is initiated at the time an application for a commission is received; and

C3.3.4.2. The applying health professional, chaplain, or attorney agrees in writing that, if the results of the investigation are unfavorable, he or she will be subject to discharge if found to be ineligible to hold a commission. Under this exception, commissions in Reserve Components other than the National Guard may be tendered to immigrant alien health professionals, chaplains, and attorneys.

C3.3.5. Mobilization of Military Retirees. The requirements contained in paragraph C3.3.2. of this section, regarding a full NAC upon reentry to active duty of any officer or enlisted regular/reserve military retiree or Individual Ready Reserve who has been separated from service for a period of greater than 12 months, should be waived for the purposes of partial or full mobilization under provisions of Title 10, (Title 14, pertaining to the U.S. Coast Guard as an element of the Navy) United States Code, to include the period of prescribed service refresher training. Particular priority should be afforded to military retirees mobilized and assigned to the defense intelligence and security agencies communities.

C3.4. SECURITY CLEARANCE

C3.4.1. General

C3.4.1.1. The authorities designated in paragraph AP5.1., Appendix 5 are the only authorities authorized to grant, deny or revoke DoD personnel security clearances. The granting of such clearances shall be limited to only those persons who require access to classified information for mission accomplishment.

C3.4.1.2. Military, DoD civilian, and contractor personnel who are employed by or serving in a consultant capacity to the Department of Defense, may be considered for access to classified information only when such access is required in connection with official duties. Such individuals may be granted either a final or interim personnel security clearance provided the investigative requirements set forth below are complied with, and provided further that all available information has been adjudicated and a finding made that such clearance would be clearly consistent with the interests of national security.

C3.4.2. Investigative Requirements for Clearance

C3.4.2.1. Top Secret

C3.4.2.1.1. Final Clearance:

C3.4.2.1.1.1. BI.

C3.4.2.1.1.2. Established billet per paragraph C3.1.5. (except contractors).

C3.4.2.1.2. Interim Clearance:

C3.4.2.1.2.1. Favorable NAC, ENTNAC, DNACI, or NACI completed.

C3.4.2.1.2.2. Favorable review of DD Form 398/SF-86/SF-171/DD Form 49.

C3.4.2.1.2.3. BI or SBI has been initiated.

C3.4.2.1.2.4. Favorable review of local personnel, base/military police, medical, and other security records as appropriate.

C3.4.2.1.2.5. Established billet per paragraph C3.1.5. (except contractors).

C3.4.2.1.2.6. Provisions of paragraph C3.2.5. have been met regarding civilian personnel.

C3.4.2.2. Secret

C3.4.2.2.1. Final Clearance:

C3.4.2.2.1.1. DNACI: Military (except first-term enlistees) and contractor employees.

C3.4.2.2.1.2. NACI: Civilian employees.

C3.4.2.2.1.3. ENTNAC: First-term enlistees.

C3.4.2.2.2. Interim Clearance:

C3.4.2.2.2.1. When a valid need to access Secret information is established, an interim Secret clearance may be issued in every case, provided that the steps outlined in subparagraphs C3.4.2.2.2. through C3.4.2.2.5., below, have been complied with.

C3.4.2.2.2.2. Favorable review of DD Form 398-2/SF-85/SF-171/DD Form 48.

C3.4.2.2.2.3. NACI, DNACI, or ENTNAC initiated.

C3.4.2.2.2.4. Favorable review of local personnel, base military police, medical, and security records as appropriate.

C3.4.2.2.2.5. Provisions of paragraph C3.2.5. have been complied with regarding civilian personnel.

C3.4.2.2.3. Confidential

C3.4.2.2.3.1. Final Clearance:

C3.4.2.2.3.1.1. NAC or ENTNAC: Military and contractor employees (except for Philippine national members of the United States Navy on whom a BI shall be favorably completed).

C3.4.2.2.3.1.2. NACI: Civilian employees (except for summer hires who may be granted a final clearance on the basis of a NAC).

C3.4.2.2.3.2. Interim Clearance

C3.4.2.2.3.2.1. Favorable review of DD Form 398-2/SF 85/SF 17 1/DD Form 48.

C3.4.2.2.3.2.2. NAC, ENTNAC or NACI initiated.

C3.4.2.2.3.2.3. Favorable review of local personnel, base military police, medical, and security records as appropriate.

C3.4.2.2.3.2.4. Provisions of paragraph C3.2.5. have been complied with regarding civilian personnel.

C3.4.2.2.4. Validity of Previously Granted Clearances: Clearances granted under less stringent investigative requirements retain their validity; however, if a

| C3.4.5. Restrictions on Issuance of Personnel Security Clearance. Personnel security clearances must be kept to the absolute minimum necessary to meet mission requirements.

| **Personnel security clearances shall normally not be issued:**

 C3.4.5.1. To persons in nonsensitive positions.

 C3.4.5.2. To persons whose regular duties do not require authorized access to classified information.

 C3.4.5.3. For ease of movement of persons within a restricted, controlled, or industrial area, whose duties do not require access to classified information.

 C3.4.5.4. To persons who may only have inadvertent access to sensitive information or areas, such as guards, emergency service personnel firemen, doctors, nurses, police, ambulance drivers, or similar personnel.

 C3.4.5.5. To persons working in shipyards whose duties do not require access to classified information.

 C3.4.5.6. To persons who can be prevented from accessing classified information by being escorted by cleared personnel.

 C3.4.5.7. To food service personnel, vendors and similar commercial sales or service personnel whose duties do not require access to classified information.

 C3.4.5.8. To maintenance or cleaning personnel who may only have inadvertent access to classified information unless such access cannot be reasonably prevented.

 C3.4.5.9. To persons who perform maintenance on office equipment, computers, typewriters, and similar equipment who can be denied classified access by physical security measures.

 C3.4.5.10. To perimeter security personnel who have no access to classified information.

 C3.4.5.11. To drivers, chauffeurs and food service personnel.

| C3.4.6. Dual Citizenship. Persons claiming both United States and foreign

citizenship shall be processed: under paragraph C3.4.2., above, and adjudicated in accordance with the "Foreign Preference" standard in Appendix 8.

| C3.4.7. **One-Time Access**. Circumstances may arise where an urgent operational or contractual exigency exists for cleared DoD personnel to have one-time or short duration access to classified information at a higher level than is authorized by the existing security clearance. In many instances, the processing time required to upgrade the clearance would preclude timely access to the information. In such situations, and only for compelling reasons in furtherance of the DoD mission, an authority referred to in subparagraph C3.4.7.1., below, may grant higher level access on a temporary basis subject to the terms and conditions prescribed below. This special authority may be revoked for abuse, inadequate record keeping, or inadequate security oversight. These procedures do not apply when circumstances exist which would permit the routine processing of an individual for the higher level clearance. Procedures and conditions for effecting emergency one-time access to the next higher classification level are as follows:

 C3.4.7.1. Authorization for such one-time access shall be granted by a flag or general officer, a general court martial convening authority or equivalent Senior Executive Service member, after coordination with appropriate security officials.

 C3.4.7.2. The recipient of the one-time access authorization must be a U.S. citizen, possess a current DoD security clearance, and the access required shall be limited to classified information one level higher than the current clearance.

 C3.4.7.3. Such access, once granted, shall be canceled promptly when no longer required, at the conclusion of the authorized period of access, or upon notification from the granting authority.

 C3.4.7.4. The employee to be afforded the higher level access shall have been continuously employed by a DoD Component or a cleared DoD contractor for the preceding 24-month period. Higher level access is not authorized for part-time employees.

 C3.4.7.5. Pertinent local records concerning the employee concerned shall be reviewed with favorable results.

 C3.4.7.6. Whenever possible, access shall be confined to a single instance or at most, a few occasions. The approval for access shall automatically expire 30 calendar days from date access commenced. If the need for access is expected to continue for a period in excess of 30 days, written approval of the granting authority is

required. At such time as it is determined that the need for access is expected to extend beyond 90 days, the individual concerned shall be promptly processed for the level of clearance required. When extended access has been approved, such access shall be canceled at or before 90 days from original date of access.

C3.4.7.7. Access at the higher level shall be limited to information under the control and custody of the authorizing official and shall be afforded under the general supervision of a properly cleared employee. The employee charged with providing such supervision shall be responsible for:

- C3.4.7.7.1. Recording the higher-level information actually revealed,
- C3.4.7.7.2. The date(s) such access is afforded, and
- C3.4.7.7.3. The daily retrieval of the material accessed.

C3.4.7.8. Access at the next higher level shall not be authorized for COMSEC, SCI, NATO, or foreign government information.

C3.4.7.9. The exercise of this provision shall be used sparingly and repeat use within any 12 month period on behalf of the same individual is prohibited. The approving authority shall maintain a record containing the following data with respect to each such access approved:

C3.4.7.9.1. The name, and SSN of the employee afforded higher level access.

C3.4.7.9.2. The level of access authorized.

C3.4.7.9.3. Justification for the access, to include an explanation of the compelling reason to grant the higher level access and specifically how the DoD mission would be furthered.

C3.4.7.9.4. An unclassified description of the specific information to which access was authorized and the duration of access along with the date(s) access was afforded.

C3.4.7.9.5. A listing of the local records reviewed and a statement that no significant adverse information concerning the employee is known to exist.

C3.4.7.9.6. The approving authority's signature certifying C3.4.7.9.1. through C3.4.7.9.5., above.

C6. CHAPTER 6
ADJUDICATION

C6.1. ADJUDICATION

C6.1.1. General

C6.1.1.1. The standard that must be met for clearance or assignment to sensitive duties is that, based on all available information, the person's loyalty, reliability, and trustworthiness are such that entrusting the person with classified information or assigning the person to sensitive duties is clearly consistent with the interests of national security.

C6.1.1.2. The principal objective of the DoD personnel security adjudicative function, consequently, is to assure selection of persons for sensitive positions who meet this standard. The adjudication process involves the effort to assess the probability of future behavior, which could have an effect adverse to the national security. Since few, if any, situations allow for positive, conclusive evidence of certain future conduct, it is an attempt to judge whether the circumstances of a particular case, taking into consideration prior experience with similar cases, reasonably suggest a degree of probability of prejudicial behavior not consistent with the national security. It is invariably a subjective determination, considering the past but necessarily anticipating the future. Rarely is proof of trustworthiness and reliability or untrustworthiness and unreliability beyond all reasonable doubt.

C6.1.1.3. Establishing relevancy is one of the key objectives of the personnel security adjudicative process in evaluating investigative material. It involves neither the judgment of criminal guilt nor the determination of general suitability for a given position; rather, it is the assessment of a person's trustworthiness and fitness for a responsibility that could, if abused, have unacceptable consequences for the national security.

C6.1.1.4. While equity demands optimal uniformity in evaluating individual cases, assuring fair and consistent assessment of circumstances from one situation to the next, each case must be weighed on its own merits, taking into consideration all relevant facts, and prior experience in similar cases. All information of record, both

favorable and unfavorable, must be considered and assessed in terms of accuracy, completeness, relevance, seriousness, and overall significance. In all adjudications the protection of the national security shall be the paramount determinant.

C6.1.2. Central Adjudication

C6.1.2.1. To ensure uniform application of the requirement of this Regulation and to ensure that DoD personnel security determinations are effected consistent with existing statutes and Executive orders, the Head of each Military Department and Defense Agencies shall establish a single Central Adjudication Facility for his/her component. The function of such facility shall be limited to evaluating personnel security investigations and making personnel security determinations. The chief of each Central Adjudication Facility shall have the authority to act on behalf of the Head of the Component concerned with respect to personnel security determinations. All information relevant to determining whether a person meets the appropriate personnel security standard prescribed by this Regulation shall be reviewed and evaluated by personnel security specialists specifically designated by the Head of the Component concerned, or designee.

C6.1.2.2. In view of the significance each adjudicative decision can have on a person's career and to ensure the maximum degree of fairness and equity in such actions, a minimum level of review shall be required for all clearance/access determinations related to the following categories of investigations:

C6.1.2.2.1. BI/SBI/PR/ENAC/SII:

C6.1.2.2.1.1. Favorable: Completely favorable investigations shall be reviewed and approved by an adjudicative official in the civilian grade of GS-7/9 or the military rank of O-3.

C6.1.2.2.1.2. Unfavorable: Investigations that are not completely favorable shall undergo at least two levels of review by adjudicative officials, the second of which must be at the civilian grade of GS-11/12 or the military rank of O-4. When an unfavorable administrative action is contemplated under paragraph C8.2.2., the letter of intent (LOI) to deny or revoke must be approved and signed by an adjudicative official at the civilian grade of GS-13/14 or the military rank of O-5. A final notification of unfavorable administrative action, subsequent to the issuance of the LOI, must be approved and signed at the civilian grade of GS-14/15 or the military rank of O-6.

C6.1.2.2.2. NACI/DNACI/NAC/ENTNAC:

C6.1.2.2.2.1. Favorable: A completely favorable investigation may be finally adjudicated after one level of review provided that the decision making authority is at the civilian grade of GS-5/7 or the military rank of O-2.

C6.1.2.2.2.2. Unfavorable: Investigations that are not completely favorable must be reviewed by an adjudicative official in the civilian grade of GS-7/9 or the military rank of O-3. When an unfavorable administrative action is contemplated under paragraph C8.2.2., the letter of intent to deny/ revoke must be signed by an adjudicative official at the civilian grade of GS-11/12 or the military rank of O-4. A final notification of unfavorable administrative action subsequent to the issuance of the LOI must be signed by an adjudicative official at the civilian grade of GS-13 or the military rank of O-5 or above.

C6.1.2.2.3. Exceptions to the above policy may only be granted by the Deputy Under Secretary of Defense for Policy.

C6.1.3. Evaluation of Personnel Security Information

C6.1.3.1. The criteria and adjudicative policy to be used in applying the principles at paragraph C6.1.1., above, are set forth in paragraph C2.2.1. and Appendix 8 of this Regulation. The ultimate consideration in making a favorable personnel security determination is whether such determination is clearly consistent with the interests of national security and shall be an overall common sense evaluation based on all available information. Such a determination shall include consideration of the following factors:

C6.1.3.1.1. The nature and seriousness of the conduct;

C6.1.3.1.2. The circumstances surrounding the conduct;

C6.1.3.1.3. The frequency and recency of the conduct;

C6.1.3.1.4. The age of the individual;

C6.1.3.1.5. The voluntariness of participation; and

C6.1.3.1.6. The absence or presence of rehabilitation.

C6.1.3.2. Detailed adjudication policy guidance to assist adjudicators in determining whether a person is eligible for access to classified information or assignment to sensitive duties is contained in Appendix 8. Adjudication policy for access to SCI is contained in DCID 1/14.

C6.1.4. Adjudicative Record

C6.1.4.1. Each adjudicative determination, whether favorable or unfavorable, shall be entered into the Defense Clearance and Investigations Index (DCII) on a daily basis but in no case to exceed 5-working days from the date of determination.

C6.1.4.2. The rationale underlying each unfavorable personnel security determination to include the appeal process, and each favorable personnel security determination where the investigation or information upon which the determination was made included significant derogatory information of the type set forth in paragraph C2.2.1. and Appendix 8 of this Regulation shall be maintained in written or automated form and is subject to the provisions of DoD Directives 5400.7 (reference (aa)) and 5400.11 (reference (bb)). This information shall be maintained for a minimum of 5 years from the date of determination.

C8. CHAPTER 8UNFAVORABLE ADMINISTRATIVE ACTIONSC8.1. REQUIREMENTS

C8.1.1. General. For purposes of this Regulation, an unfavorable administrative action includes any adverse action which is taken as a result of a personnel security determination, as defined at paragraph DL1.1.2., and any unfavorable personnel security determination, as defined at paragraph DL1.1.29. This chapter is intended only to provide guidance for the internal operation of the Department of Defense and is not intended to, does not, and may not be relied upon, to create or enlarge the jurisdiction or review authority of any court or administrative tribunal, including the Merit Systems Protection Board.

C8.1.2. Referral for Action

C8.1.2.1. Whenever derogatory information related to the criteria and policy set forth in paragraph C2.2.1. and Appendix 8 of this Regulation is developed or otherwise becomes available to any DoD element, it shall be referred by the most expeditious means to the commander or the security officer of the organization to which the individual is assigned for duty. The commander or security officer of the organization to which the subject of the information is assigned shall review the information in terms of its security significance and completeness. If further information is needed to confirm or disprove the allegations, additional investigation should be requested. The commander of the duty organization shall **insure that the appropriate Central Adjudicative Facility (CAF) of the individual concerned is informed promptly concerning (1) the derogatory information developed and (2) any actions taken or anticipated with respect thereto**. However, referral of derogatory information to the commander or security officer **shall in no way affect or limit the responsibility of the CAF to continue to process the individual for denial or revocation of clearance or access to classified information, in accordance with paragraph C8.2.2., below, if such action is warranted and supportable by the criteria and policy contained in paragraph C2.2.1. and Appendix 8.** No unfavorable administrative action as defined in paragraphs DL1.1.28. and DL1.1.29. may be taken by the organization to which the individual is assigned for duty without affording the person the full range of protections contained in paragraph C8.2.2., below, or, in the case of SCI, Annex B, DCID 1/14 (reference (1)).

C8.1.2.2. The Director DIS shall establish appropriate alternative means whereby information with potentially serious security significance can be reported other

than through DoD command or industrial organization channels. Such access shall include utilization of the DoD Inspector General "hotline" to receive such reports for appropriate follow-up by DIS. DoD Components and industry will assist DIS in publicizing the availability of appropriate reporting channels. Additionally, DoD Components will augment the system when and where necessary. Heads of DoD Components will be notified immediately to take action if appropriate.

C8.1.3. Suspension.

C8.1.3.1. The commander or head of the organization shall determine whether, on the basis of all facts available upon receipt of the initial derogatory information, it is in the interests of national security to continue subjects security status unchanged or to take interim action to suspend subjects access to classified information or assignment to sensitive duties (or other duties requiring a trustworthiness determination), if information exists which raises serious questions as to the individual's ability or intent to protect classified information or execute sensitive duties (or other duties requiring a trustworthiness determination) until a final determination is made by the appropriate authority designated in Appendix 5.

C8.1.3.2. Whenever a determination is made to suspend a security clearance for access to classified information or assignment to sensitive duties (or other duties requiring a trustworthiness determination), **the individual concerned must be notified of the determination in writing by the commander, or component CAF, to include a brief statement of the reason(s) for the suspension action consistent with the interests of national security.**

C8.1.3.3. Component field elements must promptly report all suspension actions to the appropriate CAF, **but not later than 10 working days from the date of the suspension action. The adjudicative authority will immediately update the DCII Eligibility and Access fields to alert all users to the individual's changed status.**

C8.1.3.4. Every effort shall be made to resolve suspension cases as expeditiously as circumstances permit suspension cases exceeding 180 days shall be closely monitored and managed by the DoD Component concerned until finally resolved. Suspension cases pending in excess of 12 months will be **reported to the DASD (I&S) for review and appropriate action.**

C8.1.3.5. A final security clearance eligibility determination shall be made for all suspension actions and the determination entered in the DCII. If, however, the individual under suspension leaves the jurisdiction of the Department of Defense and no longer requires a clearance (or trustworthiness determination), entry of the "Z" Code

(adjudication action incomplete due to loss of jurisdiction) in the clearance eligibility field is appropriate. In no case shall a "suspension" code (Code Y) remain a permanent record in the DCII

C8.1.3.6. A clearance or access entry in the DCII shall not be suspended or downgraded based solely on the fact that a periodic reinvestigation was not conducted precisely within the 5-year time period for TOP SECRET/SCI or within the period prevailing for SECRET clearances under departmental policy. While every effort should be made to ensure that PRs are conducted within the prescribed timeframe, agencies must be flexible in their administration of this aspect of the personnel security program so as not to undermine the ability of the Department of Defense to accomplish its mission.

C8.1.4. Final Unfavorable Administrative Actions. The authority to make personnel security determinations that will result in an unfavorable administrative action is limited to those authorities designated in Appendix 5, except that the authority to terminate the employment of a civilian employee of a Military Department or Defense Agency is vested solely in the head of the DoD Component concerned and in such other statutory official as may be designated. Action to terminate civilian employees of the Office of the Secretary of Defense and DoD Components, on the basis of criteria listed in paragraph C2.2.1., C2.2.1.1. through C2.2.1.6., shall be coordinated with the of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence OASD(C3I) prior to final action by the Head of the DoD Component. DoD civilian employees or members of the Armed Forces shall not be removed from employment or separated from the Service under provisions of this regulation if removal or separation can be effected under OPM regulations or administrative (nonsecurity) regulations of the Military Departments. However, actions contemplated in this regard shall not affect or limit the responsibility of the CAF to continue to process the individual for clearance, access to classified information, or assignment to a sensitive position if warranted and supportable by the criteria and standards contained in this Regulation.

C8.2. PROCEDURES

C8.2.1. General. No final unfavorable personnel security clearance or access determination shall be made on a Armed Forces, an employee of the Department of Defense, a consultant to the Department of Defense, or any other person affiliated with the Department of Defense without granting the individual concerned the procedural benefits set forth in C8.2.2., below, when such determination results in an unfavorable administrative action (see paragraph C8.1.1.). As an exception, DoD contractor personnel shall be afforded the procedures contained in DoD Directive 5220.6 (reference (c)) and Red Cross/United Service Organizations employees shall be afforded the procedures prescribed by DoD Directive 5210.25 (reference (w)). Procedures for to SAPs may differ from the procedures in this Regulation as authorized in E.O. 12968 and as approved by the Secretary of Defense or Deputy Secretary of Defense.

C8.2.2. Unfavorable Administrative Action Procedures. Except as provided for below, no unfavorable administrative action shall be taken under the authority of this Regulation unless the individual concerned has been:

C8.2.2.1. Provided a written statement of the reasons (SOR) as to why the unfavorable administrative action is being taken in accordance with the example at Appendix 11, which includes sample letters and enclosures. The SOR shall be as comprehensive and detailed as the protection of sources afforded confidentiality under provisions of the Privacy Act of 1974 (reference (m)) and national security permit. The statement will contain, 1) a summary of the security concerns and supporting adverse information, 2) instructions for responding to the SOR and 3) copies of the relevant security guidelines from Appendix 8. In addition, the CAF will provide within 30 calendar days, upon request of the individual, copies of releasable records of the personnel security investigation (the CAF must retain copies of the file for at least 90 days to ensure the ready availability of the material for the subject). If the CAF is unable to provide requested documents for reasons beyond their control, then the name and address of the Agency (Agencies) to which the individual may write to obtain a copy of the records will be provided.

C8.2.2.1.1. The head of the local organization of the individual receiving an SOR shall designate a point of contact (POC) to serve as a liaison between the CAF and the individual. The duties of the POC will include, but not necessarily be limited to, delivering the SOR, having the individual acknowledge receipt of the SOR; determining whether the individual intends to respond within the time specified; ensuring that the individual understands the consequences of the proposed action as well as the to respond in a timely fashion; explaining how to obtain time extensions, procure

copies of investigative records, and the procedures for responding to the SOR; and ensuring that the individual understands that he or she can obtain legal counsel or other assistance at his or her own expense.

C8.2.2.2. Afforded an opportunity to reply in writing to the CAF within 30 calendar days from the date to submit a timely response will result in forfeiture of all future appeal rights with regard to the unfavorable administrative action. Exceptions to this policy may only be circumstances where the individual's failure to respond to the SOR was due to factors beyond his or her control. The CAF must be notified of the individual's intent to respond, via the POC, within 10-calendar days of receipt of the SOR. An extension of up to 30-calendar days may be granted by the employing organization following submission of a written request from the individual. Additional extensions may only be granted by the CAF. Responses to the CAF must be forwarded through the head of the employing organization.

C8.2.2.3. Provided a written response by the CAF to any submission under subparagraph C8.2.2.2., above. stating the final reason(s) for the unfavorable administrative action, which shall be as specific as privacy and national security considerations permit and in accordance with the example of a letter of denial (IOD) and its enclosures at Appendix 11. Such response shall be as prompt as individual circumstances permit, not to exceed 60-calendar days from the date of receipt of the response submitted under subparagraph C8.2.2.2., above, provided no additional investigative action is necessary. If a final response cannot be completed within the time frame allowed, the individual must be notified in writing of this fact, the reasons therefor, and the date a final response is expected, which shall not normally exceed a total of 90 days from the date of receipt of the response under subparagraph C8.2.2.2.

C8.2.2.4. Afforded an opportunity to appeal an LOD, issued pursuant to paragraph C8.2.2.3., above to the DoD Component Personnel Security Appeals Board (PSAB). The PSAB shall consist of a minimum of three members and function in accordance with Appendix 12. If a decision is made to appeal the LOD, the individual may do so by one of the following methods:

C8.2.2.4.1. Appeal Without a Personal Appearance: Advise the PSAB within 10-calendar days of receipt of the LOD, of the intent to appeal. Within 40-calendar days of receipt of the LOD, write to the appropriate PSAB stating reasons why the LOD should be overturned and providing any additional, relevant information that may have a bearing on the final decision by the PSAB;

C8.2.2.4.2. Appeal With a Personal Appearance: Advise the Defense Office of Hearings and Appeals (DOHA) within 10-calendar days of receipt of the LOD

that a personal appearance before a DOHA Administrative Judge (AJ) is desired in order to provide additional, relevant information, which may have a bearing on the final decision by the PSAB. DOHA will promptly schedule a personal appearance and will provide a recommendation to the PSAB generally within 60 days of receipt of the requesting the personal appearance. Procedures governing the conduct of the personal appearance before a DOHA AJ are contained at Appendix 13.

C8.2.2.5. Provided a final written decision by the PSAB, including a rationale, to any submission under subparagraph C8.2.2.4., above, stating the final disposition of the appeal. This will nominally be accomplished within 60-calendar days of receipt of the written appeal from the individual if no personal appearance was requested, or within 30-calendar days from receipt of the AJ's recommendation if a personal appearance was requested.

C8.2.3. Due Process Review. The due process and appeal procedures will be reviewed one year after implementation. The above procedures will become effective no later than 120 days after the date of this change.

C8.2.4. Exceptions to Policy. Notwithstanding paragraph C8.2.2., above or any other provision of this Regulation, nothing in this Regulation shall be deemed to limit or affect the responsibility and powers of the Secretary of Defense to find that a person is unsuitable for entrance or retention in the Armed Forces, or is ineligible for a security clearance or assignment to sensitive duties, if the national security so requires, pursuant to Section 7532, Title 5, United States Code (reference (pp)). Such authority may not be delegated and may be exercised only when it is determined that the procedures prescribed in paragraph C8.2.2., above, are not appropriate. Such determination shall be conclusive.

C8.3. REINSTATEMENT OF CIVILIAN EMPLOYEES

C8.3.1. General. Any person whose civilian employment in the Department of Defense is terminated under the provisions of this Regulation shall not be reinstated or restored to duty or reemployed in the Department of Defense unless the Secretary of Defense, or the Head of a DoD Component, finds that such reinstatement, restoration, or reemployment is clearly consistent with the interests of national security. Such a finding shall be made part of the personnel security record.

C8.3.2. Reinstatement Benefits. A DoD civilian employee whose employment has been suspended or terminated under the provisions of this Regulation and who is reinstated or restored to duty under the provisions of Section 3571 of Title 5, U.S.

Code (reference (dd)) is entitled to benefits as provided for by Section 3 of Public Law 89-380 (reference (ee)).

AP5. APPENDIX 5

DoD SECURITY CLEARANCE AND/OR SCI ACCESS DETERMINATION AUTHORITIES

AP5.1. OFFICIALS AUTHORIZED TO GRANT, DENY, OR REVOKE PERSONNEL SECURITY CLEARANCES (TOP SECRET, SECRET, AND CONFIDENTIAL)

- | AP5.1.1. Secretary of Defense and/or single designee.
- | AP5.1.2. Secretary of the Army and/or single designee.¹
- | AP5.1.3. Secretary of the Navy and/or single designee.¹
- | AP5.1.4. Secretary of the Air Force and/or single designee.¹
- | AP5.1.5. Chairman of the Joint Chiefs of Staff and/or single designee.
- | AP5.1.6. Director, Washington Headquarters Services, and/or single designee.
- | AP5.1.7. Director, National Security Agency, and/or single designee.^{1, 2}
- | AP5.1.8. Director, Defense Intelligence Agency, and/or single designee.¹
- | AP5.1.9. Deputy General Counsel, Legal Counsel, OGC, and/or single designee (for contractors under the Defense Industrial Security Program (DISP))
- | AP5.1.10. Director, Defense Investigative Service, and/or single designee, (may grant security clearances only for contractor personnel under the DISP)

¹ Authority to grant, deny or revoke access to SCI is a function of the Senior Officials of the Intelligence Community (SOIC), or their designated representative, as identified in E.O. 12333 (reference (h)) and Director of Central Intelligence Directive (DCID) 1/14 (reference (l)). The authority for making SCI access determinations may also be the same official making security clearance determinations.

² Reference to the Director, NSA or single designee is not intended to infringe upon the authorities or responsibilities contained in DoD Directive 5210.45, "Personnel Security in the National Security Agency," reference (i).

AP5.2. OFFICIALS AUTHORIZED TO GRANT, DENY, OR REVOKE LAA

Officials listed in subsection AP5.1.1. through AP5.1.10., above, and the Commanders of the Combatant Commands, or their single designee, (must be at general officer, flag rank or civilian equivalent).

AP5.3. OFFICIALS AUTHORIZED TO CERTIFY PERSONNEL UNDER THEIR JURISDICTION FOR ACCESS TO CRITICAL NUCLEAR WEAPON DESIGN INFORMATION

See enclosure to DoD Directive 5210.2 (reference (z)).

AP5.4. OFFICIAL AUTHORIZED TO APPROVE PERSONNEL FOR ASSIGNMENT TO PRESIDENTIAL SUPPORT ACTIVITIES

The Executive Secretary to the Secretary of Defense and the Deputy Secretary of Defense, or designee.

AP5.5. OFFICIALS AUTHORIZED TO GRANT ACCESS TO SIOP-ESI

AP5.5.1. Director of Strategic Target Planning

AP5.5.2. Director, Joint Staff.

AP5.5.3. Chief of Staff, U.S. Army.

AP5.5.4. Chief of Naval Operations.

AP5.5.5. Chief of Staff, U.S. Air Force.

AP5.5.6. Commandant of the Marine Corps.

AP5.5.7. Commanders of the Combatant Commands.

AP5.5.8. The authority may be further delegated in writing by the officials in subsections AP5.5.1. through AP5.5.7. to the applicable subordinates.

| AP5.6. FINAL DETERMINATIONS

| Three member PSAB shall be formed under the auspices of the following officials to render final determinations when an unfavorable personnel security determination is appealed under paragraph C8.2.2.4. of this Regulation.

- | AP5.6.1. Secretary of the Army.
- | AP5.6.2. Secretary of the Air Force.
- | AP5.6.3. Secretary of the Navy.
- | AP5.6.4. Chairman of the Joint Chiefs of Staff.
- | AP5.6.5. Director, NSA.
- | AP5.6.6. Director, DIA.
- | AP5.6.7. Director, WHS.
- | AP5.6.8. General Counsel, Department of Defense (contractors only).

| AP5.7. OFFICIALS AUTHORIZED TO SUSPEND ACCESS TO CLASSIFIED INFORMATION

| AP5.7.1. Security Clearances

| AP5.7.1.1. Contractor Personnel. The Director, Counterintelligence and Security Programs; ODASD(I&S); OASD(C3I); and the Deputy General Counsel (Legal Counsel), Office of General Counsel, OSD.

| AP5.7.1.2. Military and/or Civilian Personnel. Commander and/or Agency head, Head of the Component, or adjudicative authority.

| AP5.7.2. SCI. Cognizant SOICs, or their designees.

AP5.8. OFFICIALS AUTHORIZED TO ISSUE INTERIM CLEARANCES

AP5.8.1. Interim TOP SECRET clearances may be issued by the officials listed in section AP5.1., above. That may be further delegated on determination by the Head of the Agency.

AP5.8.2. Interim SECRET and/or CONFIDENTIAL clearances may be issued by the officials listed in section AP5.1., above, as well as by organizational commanders.

AP5.9. OFFICIALS AUTHORIZED TO DESIGNATE NONAPPROPRIATED FUND POSITIONS OF TRUST

The Heads of the DoD Components, or their designees.

Code of Federal Regulations

Title 5 - Administrative Personnel

Volume: 2

Date: 2010-01-01

Original Date: 2010-01-01

Title: PART 732 - NATIONAL SECURITY POSITIONS

Context: Title 5 - Administrative Personnel. CHAPTER I - OFFICE OF PERSONNEL MANAGEMENT (CONTINUED). SUBCHAPTER B - CIVIL SERVICE REGULATIONS (CONTINUED).

Pt. 732

PART 732—NATIONAL SECURITY POSITIONS

Subpart A—Scope

Sec.

732.101 Purpose.

732.102 Definition and applicability.

Subpart B—Designation and Investigative Requirements

732.201 Sensitivity level designations and investigative requirements.

732.202 Waivers and exceptions to investigative requirements.

732.203 Periodic reinvestigation requirements.

Subpart C—Due Process and Reporting

732.301 Due process.

732.302 Reporting to OPM.

Subpart D—Security and Related Determinations

732.401 Reemployment eligibility of certain former Federal employees.

Authority: 5 U.S.C. 3301, 3302, 7312; 50 U.S.C. 403; E.O. 10450, 3 CFR, 1949-1953 Comp., p. 936.

Source: 56 FR 18654, Apr. 23, 1991, unless otherwise noted.

Subpart A—Scope

§ 732.101 Purpose.

This part sets forth certain requirements and procedures which each agency shall observe for determining national security positions pursuant to Executive Order 10450—Security Requirements for Government Employment (April 27, 1953), 18 FR 2489, 3 CFR 1949-1953 Comp., p. 936, as amended.

§ 732.102 Definition and applicability.

(a) For purposes of this part, the term “national security position” includes:

(1) Those positions that involve activities of the Government that are concerned with the protection of the nation from foreign aggression or espionage, including development of defense plans or policies, intelligence or counterintelligence activities, and related activities concerned with the preservation of the military strength of the United States; and

(2) Positions that require regular use of, or access to, classified information. Procedures and guidance provided in OPM issuances apply.

(b) The requirements of this part apply to competitive service positions, and to Senior Executive Service positions filled by career appointment, within the Executive Branch, and agencies may apply them to

excepted service positions within the Executive Branch.

[56 FR 18654, Apr. 23, 1991, as amended at 66 FR 66711, Dec. 27, 2001]

Subpart B—Designation and Investigative Requirements

§ 732.201 Sensitivity level designations and investigative requirements.

(a) For purposes of this part, the head of each agency shall designate, or cause to be designated, any position within the department or agency the occupant of which could bring about, by virtue of the nature of the position, a material adverse effect on the national security as a sensitive position at one of three sensitivity levels: Special-Sensitive, Critical-Sensitive, or Noncritical-Sensitive.

(b) Investigative requirements for each sensitivity level are provided in OPM issuances.

[56 FR 18654, Apr. 23, 1991, as amended at 66 FR 66711, Dec. 27, 2001]

§ 732.202 Waivers and exceptions to investigative requirements.

(a) *Waivers*—(1) *General*. A waiver of the preappointment investigative requirement contained in section 3(b) of Executive Order 10450 for employment in a sensitive national security position may be made only for a limited period: (i) In case of emergency if the head of the department or agency concerned finds that such action is necessary in the national interest; and (ii) when such finding is made a part of the records of the department or agency.

(2) *Specific waiver requirements*. (i) The preappointment investigative requirement may not be waived for appointment to positions designated Special-Sensitive under this part.

(ii) For positions designated Critical-Sensitive under this part, the records of the department or agency required by § 732.202(a)(1) of this part shall show what decision was made on obtaining prewaiver checks, as follows: (A) The nature of the emergency precluded obtaining prewaiver checks; or (B) checks were initiated but not all responses were received within 5 days; or (C) checks made and favorably completed are listed.

(iii) The waiver restriction is optional for positions designated Noncritical-Sensitive under this part.

(iv) When waiver is authorized, the required investigation must be initiated within 14 days of placement of the individual in the position.

(b) *Exceptions to investigative requirements*. (1) Pursuant to section 3(a) of E.O. 10450, the following positions are exempt from the investigative requirements of E.O. 10450, providing that the employing agency conducts such checks as it deems appropriate to insure that the employment or retention of individuals in these positions is clearly consistent with the interests of the national security:

(i) Positions that are intermittent, seasonal, per diem, or temporary, not to exceed an aggregate of 180 days in either a single continuous appointment or series of appointments; or

(ii) Positions filled by aliens employed outside the United States.

(2) Other positions that OPM, in its discretion, deems appropriate may be made exempt based on a written request to OPM by the agency head in whose department or agency the positions are located.

§ 732.203 Periodic reinvestigation requirements.

The incumbent of each position designated Special-Sensitive or Critical-Sensitive under this part shall be subject to periodic reinvestigation of a scope prescribed by OPM 5 years after placement, and at least once each succeeding 5 years. The employing agency will use the results of such periodic reinvestigation to determine whether the continued employment of the individual in a sensitive position is clearly consistent with the interests of the national security.

Subpart C—Due Process and Reporting

§ 732.301 Due process.

When an agency makes an adjudicative decision under this part based on an OPM investigation, or when an agency, as a result of information in an OPM investigation, changes a tentative favorable placement or clearance decision to an unfavorable decision, the agency must:

Executive Order 10450--Security requirements for Government employment

Source: The provisions of Executive Order 10450 of Apr. 27, 1953, appear at 18 FR 2489, 3 CFR, 1949-1953 Comp., p. 936, unless otherwise noted.

WHEREAS the interests of the national security require that all persons privileged to be employed in the departments and agencies of the Government, shall be reliable, trustworthy, of good conduct and character, and of complete and unswerving loyalty to the United States; and

WHEREAS the American tradition that all persons should receive fair, impartial, and equitable treatment at the hands of the Government requires that all persons seeking the privilege of employment or privileged to be employed in the departments and agencies of the Government be adjudged by mutually consistent and no less than minimum standards and procedures among the departments and agencies governing the employment and retention in employment of persons in the Federal service:

NOW, THEREFORE, by virtue of the authority vested in me by the Constitution and statutes of the United States, including section 1753 of the Revised Statutes of the United States (5 U.S.C. 631); the Civil Service Act of 1883 (22 Stat. 403; 5 U.S.C. 632, et seq.); section 9A of the act of August 2, 1939, 53 Stat. 1148 (5 U.S.C. 118j); and the act of August 26, 1950, 64 Stat. 476 (5 U.S.C. 22-1, et seq.), and as President of the United States, and deeming such action necessary in the best interests of the national security, it is hereby ordered as follows:

Section 1. In addition to the departments and agencies specified in the said act of August 26, 1950, and Executive Order No. 10237 of April 26, 1951, the provisions of that act shall apply to all other departments and agencies of the Government.¹

Sec. 2. The head of each department and agency of the Government shall be responsible for establishing and maintaining within his department or agency an effective program to insure that the employment and retention in employment of any civilian officer or employee within the department or agency is clearly consistent with the interests of the national security.

Sec. 3. (a) The appointment of each civilian officer or employee in any department or agency of the Government shall be made subject to investigation. The scope of the investigation shall be determined in the first instance according to the degree of adverse effect the occupant of the position sought to be filled could bring about, by virtue of the nature of the position, on the national security, but in no event shall the investigation include less than a national agency check (including a check of the fingerprint files of the Federal Bureau of Investigation), and written inquiries to appropriate local law-enforcement agencies, former employers and supervisors, references, and schools attended by the person under investigation: *Provided*, that upon request of the head of the department or agency concerned, the Office of Personnel Management may, in its discretion, authorize such less investigation as may meet the requirements of the national security with respect to per-diem, intermittent, temporary, or seasonal employees, or aliens employed outside the United States. Should there develop at any stage of investigation information indicating that the employment of any such person may not be clearly consistent with the interests of the national security, there shall be conducted with respect to such person a

full field investigation, or such less investigation as shall be sufficient to enable the head of the department or agency concerned to determine whether retention of such person is clearly consistent with the interests of the national security.

(b) The head of any department or agency shall designate, or cause to be designated, any position within his department or agency the occupant of which could bring about, by virtue of the nature of the position, a material adverse effect on the national security as a sensitive position. Any position so designated shall be filled or occupied only by a person with respect to whom a full field investigation has been conducted: *Provided*, that a person occupying a sensitive position at the time it is designated as such may continue to occupy such position pending the completion of a full field investigation, subject to the other provisions of this order: *And provided further*, that in case of emergency a sensitive position may be filled for a limited period by a person with respect to whom a full field pre-appointment investigation has not been completed if the head of the department or agency concerned finds that such action is necessary in the national interest, which finding shall be made a part of the records of such department or agency.

[Sec. 3 amended by EO 12107 of Dec. 28, 1978, 44 FR 1055, 3 CFR, 1978 Comp., p. 264]

Sec. 4. The head of each department and agency shall review, or cause to be reviewed, the cases of all civilian officers and employees with respect to whom there has been conducted a full field investigation under Executive Order No. 9835 of March 21, 1947, and, after such further investigation as may be appropriate, shall re-adjudicate, or cause to be re-adjudicated, in accordance with the said act of August 26, 1950, such of those cases as have not been adjudicated under a security standard commensurate with that established under this order.

Sec. 5. Whenever there is developed or received by any department or agency information indicating that the retention in employment of any officer or employee of the Government may not be clearly consistent with the interests of the national security, such information shall be forwarded to the head of the employing department or agency or his representative, who, after such investigation as may be appropriate, shall review, or cause to be reviewed, and, where necessary, re-adjudicate, or cause to be re-adjudicated, in accordance with the said act of August 26, 1950, the case of such officer or employee.

Sec. 6. Should there develop at any stage of investigation information indicating that the employment of any officer or employee of the Government may not be clearly consistent with the interests of the national security, the head of the department or agency concerned or his representative shall immediately suspend the employment of the person involved if he deems such suspension necessary in the interests of the national security and, following such investigation and review as he deems necessary, the head of the department or agency concerned shall terminate the employment of such suspended officer or employee whenever he shall determine such termination necessary or advisable in the interests of the national security, in accordance with the said act of August 26, 1950.

Sec. 7. Any person whose employment is suspended or terminated under the authority granted to heads of departments and agencies by or in accordance with the said act of August 26, 1950, or pursuant to the said Executive Order No. 9835 or any other security or loyalty program relating to officers or employees of the Government, shall not be reinstated or restored to duty or

reemployed in the same department or agency and shall not be reemployed in any other department or agency, unless the head of the department or agency concerned finds that such reinstatement, restoration, or reemployment is clearly consistent with the interests of the national security, which finding shall be made a part of the records of such department or agency: *Provided*, that no person whose employment has been terminated under such authority thereafter may be employed by any other department or agency except after a determination by the Office of Personnel Management that such person is eligible for such employment.

[Sec. 7 amended by EO 12107 of Dec. 28, 1978, 44 FR 1055, 3 CFR, 1978 Comp., p. 264]

Sec. 8. (a) The investigations conducted pursuant to this order shall be designed to develop information as to whether the employment or retention in employment in the Federal service of the person being investigated is clearly consistent with the interests of the national security. Such information shall relate, but shall not be limited, to the following:

- (1) Depending on the relation of the Government employment to the national security:
 - (i) Any behavior, activities, or associations which tend to show that the individual is not reliable or trustworthy.
 - (ii) Any deliberate misrepresentations, falsifications, or omissions of material facts.
 - (iii) Any criminal, infamous, dishonest, immoral, or notoriously disgraceful conduct, habitual use of intoxicants to excess, drug addiction, sexual perversion.
 - (iv) Any illness, including any mental condition, of a nature which in the opinion of competent medical authority may cause significant defect in the judgment or reliability of the employee, with due regard to the transient or continuing effect of the illness and the medical findings in such case.
 - (v) Any facts which furnish reason to believe that the individual may be subjected to coercion, influence, or pressure which may cause him to act contrary to the best interests of the national security.
- (2) Commission of any act of sabotage, espionage, treason, or sedition, or attempts thereat or preparation therefore, or conspiring with, or aiding or abetting, another to commit or attempt to commit any act of sabotage, espionage, treason, or sedition.
- (3) Establishing or continuing a sympathetic association with a saboteur, spy, traitor, seditionist, anarchist, or revolutionist, or with an espionage or other secret agent or representative of a foreign nation, or any representative of a foreign nation whose interests may be inimical to the interests of the United States, or with any person who advocates the use of force or violence to overthrow the government of the United States or the alteration of the form of government of the United States by unconstitutional means.
- (4) Advocacy of use of force or violence to overthrow the government of the United States, or of the alteration of the form of government of the United States by unconstitutional means.
- (5) Knowing membership with the specific intent of furthering the aims of, or adherence to and active participation in, any foreign or domestic organization, association, movement, group, or combination of persons (hereinafter referred to as organizations) which unlawfully advocates or practices the commission of acts of force or violence to prevent others from exercising their rights under the Constitution or laws of the United

States or of any State, or which seeks to overthrow the Government of the United States or any State or subdivision thereof by unlawful means.

(6) Intentional, unauthorized disclosure to any person of security information, or of other information disclosure of which is prohibited by law, or willful violation or disregard of security regulations.

(7) Performing or attempting to perform his duties, or otherwise acting, so as to serve the interests of another government in preference to the interests of the United States.

(8) Refusal by the individual, upon the ground of constitutional privilege against self-incrimination, to testify before a congressional committee regarding charges of his alleged disloyalty or other misconduct.

(b) The investigation of persons entering or employed in the competitive service shall primarily be the responsibility of the Office of Personnel Management, except in cases in which the head of a department or agency assumes that responsibility pursuant to law or by agreement with the Office. The Office shall furnish a full investigative report to the department or agency concerned.

(c) The investigation of persons (including consultants, however employed), entering employment of, or employed by, the Government other than in the competitive service shall primarily be the responsibility of the employing department or agency. Departments and agencies without investigative facilities may use the investigative facilities of the Office of Personnel Management, and other departments and agencies may use such facilities under agreement with the Office.

(d) There shall be referred promptly to the Federal Bureau of Investigation all investigations being conducted by any other agencies which develop information indicating that an individual may have been subjected to coercion, influence, or pressure to act contrary to the interests of the national security, or information relating to any of the matters described in subdivisions (2) through (8) of subsection (a) of this section. In cases so referred to it, the Federal Bureau of Investigation shall make a full field investigation.

[Sec. 8 amended by EO 10491 of Oct. 13, 1953, 18 FR 6583, 3 CFR, 1949-1953 Comp., p. 973; EO 10531 of May 27, 1954, 19 FR 3069, 3 CFR, 1954-1958 Comp., p. 193; EO 10548 of Aug. 2, 1954, 19 FR 4871, 3 CFR, 1954-1958 Comp., p. 200; EO 11785 of June 4, 1974, 39 FR 20053, 3 CFR, 1971-1975 Comp., p. 874; EO 12107 of Dec. 28, 1978, 44 FR 1055, 3 CFR, 1978 Comp., p. 264]

Sec. 9. (a) There shall be established and maintained in the Office of Personnel Management a security-investigations index covering all persons as to whom security investigations have been conducted by any department or agency of the Government under this order. The central index established and maintained by the Office under Executive Order No. 9835 of March 21, 1947, shall be made a part of the security-investigations index. The security-investigations index shall contain the name of each person investigated, adequate identifying information concerning each such person, and a reference to each department and agency which has conducted an investigation concerning the person involved or has suspended or terminated the employment of such person under the authority granted to heads of departments and agencies by or in accordance with the said act of August 26, 1950.

(b) The heads of all departments and agencies shall furnish promptly to the Office of Personnel Management information appropriate for the establishment and maintenance of the security-investigations index.

(c) The reports and other investigative material and information developed by investigations conducted pursuant to any statute, order, or program described in section 7 of this order shall remain the property of the investigative agencies conducting the investigations, but may, subject to considerations of the national security, be retained by the department or agency concerned. Such reports and other investigative material and information shall be maintained in confidence, and no access shall be given thereto except, with the consent of the investigative agency concerned, to other departments and agencies conducting security programs under the authority granted by or in accordance with the said act of August 26, 1950, as may be required for the efficient conduct of Government business.

[Sec. 9 amended by EO 12107 of Dec. 28, 1978, 44 FR 1055, 3 CFR, 1978 Comp., p. 264]

Sec. 10. Nothing in this order shall be construed as eliminating or modifying in any way the requirement for any investigation or any determination as to security which may be required by law.

Sec. 11. On and after the effective date of this order the Loyalty Review Board established by Executive Order No. 9835 of March 21, 1947, shall not accept agency findings for review, upon appeal or otherwise. Appeals pending before the Loyalty Review Board on such date shall be heard to final determination in accordance with the provisions of the said Executive Order No. 9835, as amended. Agency determinations favorable to the officer or employee concerned pending before the Loyalty Review Board on such date shall be acted upon by such Board, and whenever the Board is not in agreement with such favorable determination the case shall be remanded to the department or agency concerned for determination in accordance with the standards and procedures established pursuant to this order. Cases pending before the regional loyalty boards of the Office of Personnel Management on which hearings have not been initiated on such date shall be referred to the department or agency concerned. Cases being heard by regional loyalty boards on such date shall be heard to conclusion and the determination of the board shall be forwarded to the head of the department or agency concerned: *Provided*, that if no specific department or agency is involved, the case shall be dismissed without prejudice to the applicant. Investigations pending in the Federal Bureau of Investigation or the Office of Personnel Management on such date shall be completed, and the reports thereon shall be made to the appropriate department or agency.

[Sec. 11 amended by EO 12107 of Dec. 28, 1978, 44 FR 1055, 3 CFR, 1978 Comp., p. 264]

Sec. 12. Executive Order No. 9835 of March 21, 1947, as amended, is hereby revoked.

[Sec. 12 amended by EO 11785 of June 4, 1974, 39 FR 20053, 3 CFR, 1971-1975 Comp., p. 874]

Sec. 13. The Attorney General is requested to render to the heads of departments and agencies such advice as may be requisite to enable them to establish and maintain an appropriate employee-security program.

Sec. 14. (a) The Office of Personnel Management, with the continuing advice and collaboration of representatives of such departments and agencies as the National Security Council may designate, shall make a continuing study of the manner in which this order is being implemented by the departments and agencies of the Government for the purpose of determining:

- (1) Deficiencies in the department and agency security programs established under this order which are inconsistent with the interests of, or directly or indirectly weaken, the national security.
- (2) Tendencies in such programs to deny to individual employees fair, impartial, and equitable treatment at the hands of the Government, or rights under the Constitution and laws of the United States or this order.

Information affecting any department or agency developed or received during the course of such continuing study shall be furnished immediately to the head of the department or agency concerned. The Office of Personnel Management shall report to the National Security Council, at least semiannually, on the results of such study, shall recommend means to correct any such deficiencies or tendencies, and shall inform the National Security Council immediately of any deficiency which is deemed to be of major importance.

(b) All departments and agencies of the Government are directed to cooperate with the Office of Personnel Management to facilitate the accomplishment of the responsibilities assigned to it by subsection (a) of this section.

(c) To assist the Office of Personnel Management in discharging its responsibilities under this order, the head of each department and agency shall, as soon as possible and in no event later than ninety days after receipt of the final investigative report on a civilian officer or employee subject to a full field investigation under the provisions of this order, advise the Office as to the action taken with respect to such officer or employee. The information furnished by the heads of departments and agencies pursuant to this section shall be included in the reports which the Office of Personnel Management is required to submit to the National Security Council in accordance with subsection (a) of this section. Such reports shall set forth any deficiencies on the part of the heads of departments and agencies in taking timely action under this order, and shall mention specifically any instances of noncompliance with this subsection.

[Sec. 14 amended by EO 10550 of Aug. 5, 1954, 19 FR 4981, 3 CFR, 1954-1958 Comp., p. 200; EO 12107 of Dec. 28, 1978, 44 FR 1055, 3 CFR, 1978 Comp., p. 264]

Sec. 15. This order shall become effective thirty days after the date hereof.

¹ **Editorial note:** In *Cole v. Young*, 76 S.Ct. 861 (1955), section 1 of Executive Order 10450 was held to be invalid if applied to every department and agency..

- (a) Insure that the records used in making the decision are accurate, relevant, timely, and complete to the extent reasonably necessary to assure fairness to the individual in any determination.
- (b) Comply with all applicable administrative due process requirements, as provided by law, rule, or regulation.
- (c) At a minimum, provide the individual concerned:
 - (1) Notice of the specific reason(s) for the decision; and
 - (2) An opportunity to respond; and
 - (3) Notice of appeal rights, if any.
- (d) Consider all available information in reaching its final decision.
- (e) Keep any record of the agency action required by OPM as published in its issuances.

[56 FR 18654, Apr. 23, 1991, as amended at 66 FR 66711, Dec. 27, 2001]

§ 732.302 Reporting to OPM.

- (a) In accordance with section 9(a) of E.O. 10450, each agency conducting an investigation under E.O. 10450 is required to notify OPM when the investigation is initiated.
- (b) In accordance with section 14(c) of E.O. 10450, agencies shall report to OPM the action taken with respect to individuals investigated pursuant to E.O. 10450 as soon as possible and in no event later than 90 days after receipt of the final report of investigation.

Subpart D—Security and Related Determinations

§ 732.401 Reemployment eligibility of certain former Federal employees.

- (a) *Request.* A former employee who was terminated, or who resigned while charges were pending, from a department or agency of the Government under a statute or executive order authorizing termination in the interest of national security or on grounds relating to loyalty, and authorizing OPM to determine the eligibility for employment in another department or agency of the Government, may request OPM in writing to determine whether the individual is eligible for employment in another department or agency of the Government.
- (b) *Action by OPM.* (1) OPM shall determine, and will notify the former employee, after appropriate consideration of the case, including such investigation as it considers necessary, whether the individual may be employed in another department or agency of the Government.
(2) If a former Federal employee found ineligible under this section has had an opportunity to comment on the reasons for the action, or has furnished them to OPM or to the former employing agency, OPM may cancel the reinstatement eligibility if the eligibility resulted from the last Federal employment and was obtained through fraud, and OPM may prescribe a period of debarment not to exceed 3 years.

Monday
August 7, 1995

SECRET

SECRET

Part IV

The President

**Executive Order 12968—Access to
Classified Information**

**Presidential Determination No. 95-32 of
July 28, 1995**

**Presidential Determination No. 95-33 of
July 31, 1995**

Presidential Documents

Title 3—**Executive Order 12968 of August 2, 1995****The President****Access to Classified Information**

The national interest requires that certain information be maintained in confidence through a system of classification in order to protect our citizens, our democratic institutions, and our participation within the community of nations. The unauthorized disclosure of information classified in the national interest can cause irreparable damage to the national security and loss of human life.

Security policies designed to protect classified information must ensure consistent, cost effective, and efficient protection of our Nation's classified information, while providing fair and equitable treatment to those Americans upon whom we rely to guard our national security.

This order establishes a uniform Federal personnel security program for employees who will be considered for initial or continued access to classified information.

NOW, THEREFORE, by the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

PART 1—DEFINITIONS, ACCESS TO CLASSIFIED INFORMATION, FINANCIAL DISCLOSURE, AND OTHER ITEMS

Section 1.1. Definitions. For the purposes of this order: (a) "Agency" means any "Executive agency," as defined in 5 U.S.C. 105, the "military departments," as defined in 5 U.S.C. 102, and any other entity within the executive branch that comes into the possession of classified information, including the Defense Intelligence Agency, National Security Agency, and the National Reconnaissance Office.

(b) "Applicant" means a person other than an employee who has received an authorized conditional offer of employment for a position that requires access to classified information.

(c) "Authorized investigative agency" means an agency authorized by law or regulation to conduct a counterintelligence investigation or investigation of persons who are proposed for access to classified information to ascertain whether such persons satisfy the criteria for obtaining and retaining access to such information.

(d) "Classified information" means information that has been determined pursuant to Executive Order No. 12958, or any successor order, Executive Order No. 12951, or any successor order, or the Atomic Energy Act of 1954 (42 U.S.C. 2011), to require protection against unauthorized disclosure.

(e) "Employee" means a person, other than the President and Vice President, employed by, detailed or assigned to, an agency, including members of the Armed Forces; an expert or consultant to an agency; an industrial or commercial contractor, licensee, certificate holder, or grantee of an agency, including all subcontractors; a personal services contractor; or any other category of person who acts for or on behalf of an agency as determined by the appropriate agency head.

(f) "Foreign power" and "agent of a foreign power" have the meaning provided in 50 U.S.C. 1801.

(g) "Need for access" means a determination that an employee requires access to a particular level of classified information in order to perform or assist in a lawful and authorized governmental function.

(h) "Need-to-know" means a determination made by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.

(i) "Overseas Security Policy Board" means the Board established by the President to consider, develop, coordinate and promote policies, standards and agreements on overseas security operations, programs and projects that affect all United States Government agencies under the authority of a Chief of Mission.

(j) "Security Policy Board" means the Board established by the President to consider, coordinate, and recommend policy directives for U.S. security policies, procedures, and practices.

(k) "Special access program" has the meaning provided in section 4.1 of Executive Order No. 12958, or any successor order.

Sec. 1.2. Access to Classified Information. (a) No employee shall be granted access to classified information unless that employee has been determined to be eligible in accordance with this order and to possess a need-to-know.

(b) Agency heads shall be responsible for establishing and maintaining an effective program to ensure that access to classified information by each employee is clearly consistent with the interests of the national security.

(c) Employees shall not be granted access to classified information unless they:

(1) have been determined to be eligible for access under section 3.1 of this order by agency heads or designated officials based upon a favorable adjudication of an appropriate investigation of the employee's background;

(2) have a demonstrated need-to-know; and

(3) have signed an approved nondisclosure agreement.

(d) All employees shall be subject to investigation by an appropriate government authority prior to being granted access to classified information and at any time during the period of access to ascertain whether they continue to meet the requirements for access.

(e)(1) All employees granted access to classified information shall be required as a condition of such access to provide to the employing agency written consent permitting access by an authorized investigative agency, for such time as access to classified information is maintained and for a period of 3 years thereafter, to:

(A) relevant financial records that are maintained by a financial institution as defined in 31 U.S.C. 5312(a) or by a holding company as defined in section 1101(6) of the Right to Financial Privacy Act of 1978 (12 U.S.C. 3401);

(B) consumer reports pertaining to the employee under the Fair Credit Reporting Act (15 U.S.C. 1681a); and

(C) records maintained by commercial entities within the United States pertaining to any travel by the employee outside the United States.

(2) Information may be requested pursuant to employee consent under this section where:

(A) there are reasonable grounds to believe, based on credible information, that the employee or former employee is, or may be, disclosing classified information in an unauthorized manner to a foreign power or agent of a foreign power;

(B) information the employing agency deems credible indicates the employee or former employee has incurred excessive indebtedness or has ac-

quired a level of affluence that cannot be explained by other information; or

(C) circumstances indicate the employee or former employee had the capability and opportunity to disclose classified information that is known to have been lost or compromised to a foreign power or an agent of a foreign power.

(3) Nothing in this section shall be construed to affect the authority of an investigating agency to obtain information pursuant to the Right to Financial Privacy Act, the Fair Credit Reporting Act or any other applicable law.

Sec. 1.3. *Financial Disclosure.* (a) Not later than 180 days after the effective date of this order, the head of each agency that originates, handles, transmits, or possesses classified information shall designate each employee, by position or category where possible, who has a regular need for access to classified information that, in the discretion of the agency head, would reveal:

(1) the identity of covert agents as defined in the Intelligence Identities Protection Act of 1982 (50 U.S.C. 421);

(2) technical or specialized national intelligence collection and processing systems that, if disclosed in an unauthorized manner, would substantially negate or impair the effectiveness of the system;

(3) the details of:

(A) the nature, contents, algorithm, preparation, or use of any code, cipher, or cryptographic system or;

(B) the design, construction, functioning, maintenance, or repair of any cryptographic equipment; but not including information concerning the use of cryptographic equipment and services;

(4) particularly sensitive special access programs, the disclosure of which would substantially negate or impair the effectiveness of the information or activity involved; or

(5) especially sensitive nuclear weapons design information (but only for those positions that have been certified as being of a high degree of importance or sensitivity, as described in section 145(f) of the Atomic Energy Act of 1954, as amended).

(b) An employee may not be granted access, or hold a position designated as requiring access, to information described in subsection (a) unless, as a condition of access to such information, the employee:

(1) files with the head of the agency a financial disclosure report, including information with respect to the spouse and dependent children of the employee, as part of all background investigations or reinvestigations;

(2) is subject to annual financial disclosure requirements, if selected by the agency head; and

(3) files relevant information concerning foreign travel, as determined by the Security Policy Board.

(c) Not later than 180 days after the effective date of this order, the Security Policy Board shall develop procedures for the implementation of this section, including a standard financial disclosure form for use by employees under subsection (b) of this section, and agency heads shall identify certain employees, by position or category, who are subject to annual financial disclosure.

Sec. 1.4. *Use of Automated Financial Record Data Bases.* As part of all investigations and reinvestigations described in section 1.2(d) of this order, agencies may request the Department of the Treasury, under terms and conditions prescribed by the Secretary of the Treasury, to search automated data bases consisting of reports of currency transactions by financial institutions, international transportation of currency or monetary instruments, foreign bank and financial accounts, transactions under \$10,000 that are reported as possible money laundering violations, and records of foreign travel.

Sec. 1.5. Employee Education and Assistance. The head of each agency that grants access to classified information shall establish a program for employees with access to classified information to: (a) educate employees about individual responsibilities under this order; and

(b) inform employees about guidance and assistance available concerning issues that may affect their eligibility for access to classified information, including sources of assistance for employees who have questions or concerns about financial matters, mental health, or substance abuse.

PART 2—ACCESS ELIGIBILITY POLICY AND PROCEDURE

Sec. 2.1. Eligibility Determinations. (a) Determinations of eligibility for access to classified information shall be based on criteria established under this order. Such determinations are separate from suitability determinations with respect to the hiring or retention of persons for employment by the government or any other personnel actions.

(b) The number of employees that each agency determines are eligible for access to classified information shall be kept to the minimum required for the conduct of agency functions.

(1) Eligibility for access to classified information shall not be requested or granted solely to permit entry to, or ease of movement within, controlled areas when the employee has no need for access and access to classified information may reasonably be prevented. Where circumstances indicate employees may be inadvertently exposed to classified information in the course of their duties, agencies are authorized to grant or deny, in their discretion, facility access approvals to such employees based on an appropriate level of investigation as determined by each agency.

(2) Except in agencies where eligibility for access is a mandatory condition of employment, eligibility for access to classified information shall only be requested or granted based on a demonstrated, foreseeable need for access. Requesting or approving eligibility in excess of actual requirements is prohibited.

(3) Eligibility for access to classified information may be granted where there is a temporary need for access, such as one-time participation in a classified project, provided the investigative standards established under this order have been satisfied. In such cases, a fixed date or event for expiration shall be identified and access to classified information shall be limited to information related to the particular project or assignment.

(4) Access to classified information shall be terminated when an employee no longer has a need for access.

Sec. 2.2. Level of Access Approval. (a) The level at which an access approval is granted for an employee shall be limited, and relate directly, to the level of classified information for which there is a need for access. Eligibility for access to a higher level of classified information includes eligibility for access to information classified at a lower level.

(b) Access to classified information relating to a special access program shall be granted in accordance with procedures established by the head of the agency that created the program or, for programs pertaining to intelligence activities (including special activities but not including military operational, strategic, and tactical programs) or intelligence sources and methods, by the Director of Central Intelligence. To the extent possible and consistent with the national security interests of the United States, such procedures shall be consistent with the standards and procedures established by and under this order.

Sec. 2.3 Temporary Access to Higher Levels. (a) An employee who has been determined to be eligible for access to classified information based on favorable adjudication of a completed investigation may be granted temporary access to a higher level where security personnel authorized by the agency head to make access eligibility determinations find that such access:

- (1) is necessary to meet operational or contractual exigencies not expected to be of a recurring nature;
- (2) will not exceed 180 days; and
- (3) is limited to specific, identifiable information that is made the subject of a written access record.

(b) Where the access granted under subsection (a) of this section involves another agency's classified information, that agency must concur before access to its information is granted.

Sec. 2.4. Reciprocal Acceptance of Access Eligibility Determinations. (a) Except when an agency has substantial information indicating that an employee may not satisfy the standards in section 3.1 of this order, background investigations and eligibility determinations conducted under this order shall be mutually and reciprocally accepted by all agencies.

(b) Except where there is substantial information indicating that the employee may not satisfy the standards in section 3.1 of this order, an employee with existing access to a special access program shall not be denied eligibility for access to another special access program at the same sensitivity level as determined personally by the agency head or deputy agency head, or have an existing access eligibility readjudicated, so long as the employee has a need for access to the information involved.

(c) This section shall not preclude agency heads from establishing additional, but not duplicative, investigative or adjudicative procedures for a special access program or for candidates for detail or assignment to their agencies, where such procedures are required in exceptional circumstances to protect the national security.

(d) Where temporary eligibility for access is granted under sections 2.3 or 3.3 of this order or where the determination of eligibility for access is conditional, the fact of such temporary or conditional access shall be conveyed to any other agency that considers affording the employee access to its information.

Sec. 2.5. Specific Access Requirement. (a) Employees who have been determined to be eligible for access to classified information shall be given access to classified information only where there is a need-to-know that information.

(b) It is the responsibility of employees who are authorized holders of classified information to verify that a prospective recipient's eligibility for access has been granted by an authorized agency official and to ensure that a need-to-know exists prior to allowing such access, and to challenge requests for access that do not appear well-founded.

Sec. 2.6. Access by Non-United States Citizens. (a) Where there are compelling reasons in furtherance of an agency mission, immigrant alien and foreign national employees who possess a special expertise may, in the discretion of the agency, be granted limited access to classified information only for specific programs, projects, contracts, licenses, certificates, or grants for which there is a need for access. Such individuals shall not be eligible for access to any greater level of classified information than the United States Government has determined may be releasable to the country of which the subject is currently a citizen, and such limited access may be approved only if the prior 10 years of the subject's life can be appropriately investigated. If there are any doubts concerning granting access, additional lawful investigative procedures shall be fully pursued.

(b) Exceptions to these requirements may be permitted only by the agency head or the senior agency official designated under section 6.1 of this order to further substantial national security interests.

PART 3—ACCESS ELIGIBILITY STANDARDS

Sec. 3.1. Standards. (a) No employee shall be deemed to be eligible for access to classified information merely by reason of Federal service or con-

tracting, licensee, certificate holder, or grantee status, or as a matter of right or privilege, or as a result of any particular title, rank, position, or affiliation.

(b) Except as provided in sections 2.6 and 3.3 of this order, eligibility for access to classified information shall be granted only to employees who are United States citizens for whom an appropriate investigation has been completed and whose personal and professional history affirmatively indicates loyalty to the United States, strength of character, trustworthiness, honesty, reliability, discretion, and sound judgment, as well as freedom from conflicting allegiances and potential for coercion, and willingness and ability to abide by regulations governing the use, handling, and protection of classified information. A determination of eligibility for access to such information is a discretionary security decision based on judgments by appropriately trained adjudicative personnel. Eligibility shall be granted only where facts and circumstances indicate access to classified information is clearly consistent with the national security interests of the United States, and any doubt shall be resolved in favor of the national security.

(c) The United States Government does not discriminate on the basis of race, color, religion, sex, national origin, disability, or sexual orientation in granting access to classified information.

(d) In determining eligibility for access under this order, agencies may investigate and consider any matter that relates to the determination of whether access is clearly consistent with the interests of national security. No inference concerning the standards in this section may be raised solely on the basis of the sexual orientation of the employee.

(e) No negative inference concerning the standards in this section may be raised solely on the basis of mental health counseling. Such counseling can be a positive factor in eligibility determinations. However, mental health counseling, where relevant to the adjudication of access to classified information, may justify further inquiry to determine whether the standards of subsection (b) of this section are satisfied, and mental health may be considered where it directly relates to those standards.

(f) Not later than 180 days after the effective date of this order, the Security Policy Board shall develop a common set of adjudicative guidelines for determining eligibility for access to classified information, including access to special access programs.

Sec. 3.2. Basis for Eligibility Approval. (a) Eligibility determinations for access to classified information shall be based on information concerning the applicant or employee that is acquired through the investigation conducted pursuant to this order or otherwise available to security officials and shall be made part of the applicant's or employee's security record. Applicants or employees shall be required to provide relevant information pertaining to their background and character for use in investigating and adjudicating their eligibility for access.

(b) Not later than 180 days after the effective date of this order, the Security Policy Board shall develop a common set of investigative standards for background investigations for access to classified information. These standards may vary for the various levels of access.

(c) Nothing in this order shall prohibit an agency from utilizing any lawful investigative procedure in addition to the investigative requirements set forth in this order and its implementing regulations to resolve issues that may arise during the course of a background investigation or reinvestigation.

Sec. 3.3. Special Circumstances. (a) In exceptional circumstances where official functions must be performed prior to the completion of the investigative and adjudication process, temporary eligibility for access to classified information may be granted to an employee while the initial investigation is underway. When such eligibility is granted, the initial investigation shall be expedited.

(1) Temporary eligibility for access under this section shall include a justification, and the employee must be notified in writing that further access is expressly conditioned on the favorable completion of the investigation and issuance of an access eligibility approval. Access will be immediately terminated, along with any assignment requiring an access eligibility approval, if such approval is not granted.

(2) Temporary eligibility for access may be granted only by security personnel authorized by the agency head to make access eligibility determinations and shall be based on minimum investigative standards developed by the Security Policy Board not later than 180 days after the effective date of this order.

(3) Temporary eligibility for access may be granted only to particular, identified categories of classified information necessary to perform the lawful and authorized functions that are the basis for the granting of temporary access.

(b) Nothing in subsection (a) shall be construed as altering the authority of an agency head to waive requirements for granting access to classified information pursuant to statutory authority.

(c) Where access has been terminated under section 2.1(b)(4) of this order and a new need for access arises, access eligibility up to the same level shall be reapproved without further investigation as to employees who were determined to be eligible based on a favorable adjudication of an investigation completed within the prior 5 years, provided they have remained employed by the same employer during the period in question, the employee certifies in writing that there has been no change in the relevant information provided by the employee for the last background investigation, and there is no information that would tend to indicate the employee may no longer satisfy the standards established by this order for access to classified information.

(d) Access eligibility shall be reapproved for individuals who were determined to be eligible based on a favorable adjudication of an investigation completed within the prior 5 years and who have been retired or otherwise separated from United States Government employment for not more than 2 years; provided there is no indication the individual may no longer satisfy the standards of this order, the individual certifies in writing that there has been no change in the relevant information provided by the individual for the last background investigation, and an appropriate record check reveals no unfavorable information.

Sec. 3.4. Reinvestigation Requirements. (a) Because circumstances and characteristics may change dramatically over time and thereby alter the eligibility of employees for continued access to classified information, reinvestigations shall be conducted with the same priority and care as initial investigations.

(b) Employees who are eligible for access to classified information shall be the subject of periodic reinvestigations and may also be reinvestigated if, at any time, there is reason to believe that they may no longer meet the standards for access established in this order.

(c) Not later than 180 days after the effective date of this order, the Security Policy Board shall develop a common set of reinvestigative standards, including the frequency of reinvestigations.

PART 4—INVESTIGATIONS FOR FOREIGN GOVERNMENTS

Sec. 4. Authority. Agencies that conduct background investigations, including the Federal Bureau of Investigation and the Department of State, are authorized to conduct personnel security investigations in the United States when requested by a foreign government as part of its own personnel security program and with the consent of the individual.

PART 5—REVIEW OF ACCESS DETERMINATIONS

Sec. 5.1. Determinations of Need for Access. A determination under section 2.1(b)(4) of this order that an employee does not have, or no longer has, a need for access is a discretionary determination and shall be conclusive.

Sec. 5.2. Review Proceedings for Denials or Revocations of Eligibility for Access. (a) Applicants and employees who are determined to not meet the standards for access to classified information established in section 3.1 of this order shall be:

(1) provided as comprehensive and detailed a written explanation of the basis for that conclusion as the national security interests of the United States and other applicable law permit;

(2) provided within 30 days, upon request and to the extent the documents would be provided if requested under the Freedom of Information Act (5 U.S.C. 552) or the Privacy Act (3 U.S.C. 552a), as applicable, any documents, records, and reports upon which a denial or revocation is based;

(3) informed of their right to be represented by counsel or other representative at their own expense; to request any documents, records, and reports as described in section 5.2(a)(2) upon which a denial or revocation is based; and to request the entire investigative file, as permitted by the national security and other applicable law, which, if requested, shall be promptly provided prior to the time set for a written reply;

(4) provided a reasonable opportunity to reply in writing to, and to request a review of, the determination;

(5) provided written notice of and reasons for the results of the review, the identity of the deciding authority, and written notice of the right to appeal;

(6) provided an opportunity to appeal in writing to a high level panel, appointed by the agency head, which shall be comprised of at least three members, two of whom shall be selected from outside the security field. Decisions of the panel shall be in writing, and final except as provided in subsection (b) of this section; and

(7) provided an opportunity to appear personally and to present relevant documents, materials, and information at some point in the process before an adjudicative or other authority, other than the investigating entity, as determined by the agency head. A written summary or recording of such appearance shall be made part of the applicant's or employee's security record, unless such appearance occurs in the presence of the appeals panel described in subsection (a)(6) of this section.

(b) Nothing in this section shall prohibit an agency head from personally exercising the appeal authority in subsection (a)(6) of this section based upon recommendations from an appeals panel. In such case, the decision of the agency head shall be final.

(c) Agency heads shall promulgate regulations to implement this section and, at their sole discretion and as resources and national security considerations permit, may provide additional review proceedings beyond those required by subsection (a) of this section. This section does not require additional proceedings, however, and creates no procedural or substantive rights.

(d) When the head of an agency or principal deputy personally certifies that a procedure set forth in this section cannot be made available in a particular case without damaging the national security interests of the United States by revealing classified information, the particular procedure shall not be made available. This certification shall be conclusive.

(e) This section shall not be deemed to limit or affect the responsibility and power of an agency head pursuant to any law or other Executive order to deny or terminate access to classified information in the interests

of national security. The power and responsibility to deny or terminate access to classified information pursuant to any law or other Executive order may be exercised only where the agency head determines that the procedures prescribed in subsection (a) of this section cannot be invoked in a manner that is consistent with national security. This determination shall be conclusive.

(f)(1) This section shall not be deemed to limit or affect the responsibility and power of an agency head to make determinations of suitability for employment.

(2) Nothing in this section shall require that an agency provide the procedures prescribed in subsection (a) of this section to an applicant where a conditional offer of employment is withdrawn for reasons of suitability or any other reason other than denial of eligibility for access to classified information.

(3) A suitability determination shall not be used for the purpose of denying an applicant or employee the review proceedings of this section where there has been a denial or revocation of eligibility for access to classified information.

PART 6—IMPLEMENTATION

Sec. 6.1. Agency Implementing Responsibilities. Heads of agencies that grant employees access to classified information shall: (a) designate a senior agency official to direct and administer the agency's personnel security program established by this order. All such programs shall include active oversight and continuing security education and awareness programs to ensure effective implementation of this order;

(b) cooperate, under the guidance of the Security Policy Board, with other agencies to achieve practical, consistent, and effective adjudicative training and guidelines; and

(c) conduct periodic evaluations of the agency's implementation and administration of this order, including the implementation of section 1.3(a) of this order. Copies of each report shall be provided to the Security Policy Board.

Sec. 6.2. Employee Responsibilities. (a) Employees who are granted eligibility for access to classified information shall:

(1) protect classified information in their custody from unauthorized disclosure;

(2) report all contacts with persons, including foreign nationals, who seek in any way to obtain unauthorized access to classified information;

(3) report all violations of security regulations to the appropriate security officials; and

(4) comply with all other security requirements set forth in this order and its implementing regulations.

(b) Employees are encouraged and expected to report any information that raises doubts as to whether another employee's continued eligibility for access to classified information is clearly consistent with the national security.

Sec. 6.3. Security Policy Board Responsibilities and Implementation. (a) With respect to actions taken by the Security Policy Board pursuant to sections 1.3(c), 3.1(f), 3.2(b), 3.3(a)(2), and 3.4(c) of this order, the Security Policy Board shall make recommendations to the President through the Assistant to the President for National Security Affairs for implementation.

(b) Any guidelines, standards, or procedures developed by the Security Policy Board pursuant to this order shall be consistent with those guidelines issued by the Federal Bureau of Investigation in March 1994 on Background Investigations Policy/Guidelines Regarding Sexual Orientation.

(c) In carrying out its responsibilities under this order, the Security Policy Board shall consult where appropriate with the Overseas Security Policy Board. In carrying out its responsibilities under section 1.3(c) of this order, the Security Policy Board shall obtain the concurrence of the Director of the Office of Management and Budget.

Sec. 6.4. Sanctions. Employees shall be subject to appropriate sanctions if they knowingly and willfully grant eligibility for, or allow access to, classified information in violation of this order or its implementing regulations. Sanctions may include reprimand, suspension without pay, removal, and other actions in accordance with applicable law and agency regulations.

PART 7—GENERAL PROVISIONS

Sec. 7.1. Classified Information Procedures Act. Nothing in this order is intended to alter the procedures established under the Classified Information Procedures Act (18 U.S.C. App. 1).

Sec. 7.2. General. (a) Information obtained by an agency under sections 1.2(e) or 1.3 of this order may not be disseminated outside the agency, except to:

(1) the agency employing the employee who is the subject of the records or information;

(2) the Department of Justice for law enforcement or counterintelligence purposes; or

(3) any agency if such information is clearly relevant to the authorized responsibilities of such agency.

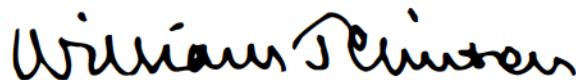
(b) The Attorney General, at the request of the head of an agency, shall render an interpretation of this order with respect to any question arising in the course of its administration.

(c) No prior Executive orders are repealed by this order. To the extent that this order is inconsistent with any provision of any prior Executive order, this order shall control, except that this order shall not diminish or otherwise affect the requirements of Executive Order No. 10450, the denial and revocation procedures provided to individuals covered by Executive Order No. 10865, as amended, or access by historical researchers and former presidential appointees under Executive Order No. 12958 or any successor order.

(d) If any provision of this order or the application of such provision is held to be invalid, the remainder of this order shall not be affected.

(e) This Executive order is intended only to improve the internal management of the executive branch and is not intended to, and does not, create any right to administrative or judicial review, or any other right or benefit or trust responsibility, substantive or procedural, enforceable by a party against the United States, its agencies or instrumentalities, its officers or employees, or any other person.

(f) This order is effective immediately.



THE WHITE HOUSE,
August 2, 1995.

[FR Doc. 95-19654]

Filed 8-4-95; 12:18 pm]

Billing code 3195-01-P

FBI investigate domestic threats in this time of war, additional funding for the Coast Guard for port security in the United States and in the Middle East.

In this time of heightened security, we are expecting States and communities to take on greater responsibilities to protect critical infrastructure. And so I'm seeking additional resources to help States and cities make these preparations for the protection of our citizens.

Yesterday I informed the leaders of Congress of these spending requests. The situation in any war is fluid. I reminded them of that fact, and so I'm asking Congress for flexibility in how these funds can be allocated. They heard that message. They also heard the message that the need is urgent. The wartime supplemental is directly related to winning this war and to securing the peace that will follow this war. I ask Congress to act quickly and responsibly.

One thing is for certain: Business as usual on Capitol Hill can't go on during this time of war. And by that I mean the supplemental should not be viewed as an opportunity to add spending that is unrelated, unwise, and unnecessary. Every dollar we spend must serve the interest of our Nation, and the interest of our Nation in this supplemental is to win this war and to be able to keep the peace.

Eighteen months ago, this building came under attack. From that day to this, we have been engaged in a new kind of war, and we are winning. We will not leave our future to be decided by terrorist groups or terrorist regimes. At every turn in this conflict, Americans can be confident in the people who wear our Nation's uniform. We support them. We are thankful for their service in places of great danger, in this hour of great need.

May God continue to look out after those who defend the peace and freedom. And may God continue to bless America. Thank you.

NOTE: The President spoke at 10:30 a.m. in the Eisenhower Dining Room. In his remarks, he referred to President Saddam Hussein of Iraq; and Gen. Tommy R. Franks, USA, combatant commander, U.S. Central Command. The Office of the Press Secretary also released a Spanish language transcript of these remarks.

Executive Order 13292—Further Amendment to Executive Order 12958, as Amended, Classified National Security Information

March 25, 2003

By the authority vested in me as President by the Constitution and the laws of the United States of America, and in order to further amend Executive Order 12958, as amended, it is hereby ordered that Executive Order 12958 is amended to read as follows:

“Classified National Security Information”

This order prescribes a uniform system for classifying, safeguarding, and declassifying national security information, including information relating to defense against transnational terrorism. Our democratic principles require that the American people be informed of the activities of their Government. Also, our Nation's progress depends on the free flow of information. Nevertheless, throughout our history, the national defense has required that certain information be maintained in confidence in order to protect our citizens, our democratic institutions, our homeland security, and our interactions with foreign nations. Protecting information critical to our Nation's security remains a priority.

Now, Therefore, by the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Part 1—Original Classification

Sec. 1.1. Classification Standards. (a) Information may be originally classified under the terms of this order only if all of the following conditions are met:

- (1) an original classification authority is classifying the information;
- (2) the information is owned by, produced by or for, or is under the control of the United States Government;
- (3) the information falls within one or more of the categories of information listed in section 1.4 of this order; and
- (4) the original classification authority determines that the unauthorized disclosure of the information reasonably

could be expected to result in damage to the national security, which includes defense against transnational terrorism, and the original classification authority is able to identify or describe the damage.

(b) Classified information shall not be declassified automatically as a result of any unauthorized disclosure of identical or similar information.

(c) The unauthorized disclosure of foreign government information is presumed to cause damage to the national security.

Sec. 1.2. Classification Levels. (a) Information may be classified at one of the following three levels:

(1) "Top Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe.

(2) "Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe.

(3) "Confidential" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe.

(b) Except as otherwise provided by statute, no other terms shall be used to identify United States classified information.

Sec. 1.3. Classification Authority. (a) The authority to classify information originally may be exercised only by:

(1) the President and, in the performance of executive duties, the Vice President;

(2) agency heads and officials designated by the President in the *Federal Register*; and

(3) United States Government officials delegated this authority pursuant to paragraph (c) of this section.

(b) Officials authorized to classify information at a specified level are also authorized to classify information at a lower level.

(c) Delegation of original classification authority.

(1) Delegations of original classification authority shall be limited to the minimum required to administer this order. Agency heads are responsible for ensuring that designated subordinate officials have a demonstrable and continuing need to exercise this authority.

(2) "Top Secret" original classification authority may be delegated only by the President; in the performance of executive duties, the Vice President; or an agency head or official designated pursuant to paragraph (a)(2) of this section.

(3) "Secret" or "Confidential" original classification authority may be delegated only by the President; in the performance of executive duties, the Vice President; or an agency head or official designated pursuant to paragraph (a)(2) of this section; or the senior agency official described in section 5.4(d) of this order, provided that official has been delegated "Top Secret" original classification authority by the agency head.

(4) Each delegation of original classification authority shall be in writing and the authority shall not be redelegated except as provided in this order. Each delegation shall identify the official by name or position title.

(d) Original classification authorities must receive training in original classification as provided in this order and its implementing directives. Such training must include instruction on the proper safeguarding of classified information and of the criminal, civil, and administrative sanctions that may be brought against an individual who fails to protect classified information from unauthorized disclosure.

(e) Exceptional cases. When an employee, government contractor, licensee, certificate holder, or grantee of an agency who does not have original classification authority

originates information believed by that person to require classification, the information shall be protected in a manner consistent with this order and its implementing directives. The information shall be transmitted promptly as provided under this order or its implementing directives to the agency that has appropriate subject matter interest and classification authority with respect to this information. That agency shall decide within 30 days whether to classify this information. If it is not clear which agency has classification responsibility for this information, it shall be sent to the Director of the Information Security Oversight Office. The Director shall determine the agency having primary subject matter interest and forward the information, with appropriate recommendations, to that agency for a classification determination.

Sec. 1.4. Classification Categories. Information shall not be considered for classification unless it concerns:

- (a) military plans, weapons systems, or operations;
- (b) foreign government information;
- (c) intelligence activities (including special activities), intelligence sources or methods, or cryptology;
- (d) foreign relations or foreign activities of the United States, including confidential sources;
- (e) scientific, technological, or economic matters relating to the national security, which includes defense against transnational terrorism;
- (f) United States Government programs for safeguarding nuclear materials or facilities;
- (g) vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security, which includes defense against transnational terrorism; or
- (h) weapons of mass destruction.

Sec. 1.5. Duration of Classification. (a) At the time of original classification, the original classification authority shall attempt to establish a specific date or event for declassification based upon the duration of the national security sensitivity of the information. Upon reaching the date or event, the information shall be automatically declassified. The date

or event shall not exceed the time frame established in paragraph (b) of this section.

(b) If the original classification authority cannot determine an earlier specific date or event for declassification, information shall be marked for declassification 10 years from the date of the original decision, unless the original classification authority otherwise determines that the sensitivity of the information requires that it shall be marked for declassification for up to 25 years from the date of the original decision. All information classified under this section shall be subject to section 3.3 of this order if it is contained in records of permanent historical value under title 44, United States Code.

(c) An original classification authority may extend the duration of classification, change the level of classification, or reclassify specific information only when the standards and procedures for classifying information under this order are followed.

(d) Information marked for an indefinite duration of classification under predecessor orders, for example, marked as "Originating Agency's Determination Required," or information classified under predecessor orders that contains no declassification instructions shall be declassified in accordance with part 3 of this order.

Sec. 1.6. Identification and Markings. (a) At the time of original classification, the following shall appear on the face of each classified document, or shall be applied to other classified media in an appropriate manner:

- (1) one of the three classification levels defined in section 1.2 of this order;
- (2) the identity, by name or personal identifier and position, of the original classification authority;
- (3) the agency and office of origin, if not otherwise evident;
- (4) declassification instructions, which shall indicate one of the following:
- (A) the date or event for declassification, as prescribed in section 1.5(a) or section 1.5(c);
- (B) the date that is 10 years from the date of original classification, as prescribed in section 1.5(b); or
- (C) the date that is up to 25 years from the date of original classification, as prescribed in section 1.5 (b); and

(5) a concise reason for classification that, at a minimum, cites the applicable classification categories in section 1.4 of this order.

(b) Specific information described in paragraph (a) of this section may be excluded if it would reveal additional classified information.

(c) With respect to each classified document, the agency originating the document shall, by marking or other means, indicate which portions are classified, with the applicable classification level, and which portions are unclassified. In accordance with standards prescribed in directives issued under this order, the Director of the Information Security Oversight Office may grant waivers of this requirement. The Director shall revoke any waiver upon a finding of abuse.

(d) Markings implementing the provisions of this order, including abbreviations and requirements to safeguard classified working papers, shall conform to the standards prescribed in implementing directives issued pursuant to this order.

(e) Foreign government information shall retain its original classification markings or shall be assigned a U.S. classification that provides a degree of protection at least equivalent to that required by the entity that furnished the information. Foreign government information retaining its original classification markings need not be assigned a U.S. classification marking provided that the responsible agency determines that the foreign government markings are adequate to meet the purposes served by U.S. classification markings.

(f) Information assigned a level of classification under this or predecessor orders shall be considered as classified at that level of classification despite the omission of other required markings. Whenever such information is used in the derivative classification process or is reviewed for possible declassification, holders of such information shall coordinate with an appropriate classification authority for the application of omitted markings.

(g) The classification authority shall, whenever practicable, use a classified addendum whenever classified information constitutes a

small portion of an otherwise unclassified document.

(h) Prior to public release, all declassified records shall be appropriately marked to reflect their declassification.

Sec. 1.7. Classification Prohibitions and Limitations. (a) In no case shall information be classified in order to:

- (1) conceal violations of law, inefficiency, or administrative error;
- (2) prevent embarrassment to a person, organization, or agency;
- (3) restrain competition; or
- (4) prevent or delay the release of information that does not require protection in the interest of the national security.

(b) Basic scientific research information not clearly related to the national security shall not be classified.

(c) Information may be reclassified after declassification and release to the public under proper authority only in accordance with the following conditions:

- (1) the reclassification action is taken under the personal authority of the agency head or deputy agency head, who determines in writing that the reclassification of the information is necessary in the interest of the national security;
- (2) the information may be reasonably recovered; and
- (3) the reclassification action is reported promptly to the Director of the Information Security Oversight Office.

(d) Information that has not previously been disclosed to the public under proper authority may be classified or reclassified after an agency has received a request for it under the Freedom of Information Act (5 U.S.C. 552) or the Privacy Act of 1974 (5 U.S.C. 552a), or the mandatory review provisions of section 3.5 of this order only if such classification meets the requirements of this order and is accomplished on a document-by-document basis with the personal participation or under the direction of the agency head, the deputy agency head, or the senior agency official designated under section 5.4 of this order.

(e) Compilations of items of information that are individually unclassified may be classified if the compiled information reveals an additional association or relationship that: (1) meets the standards for classification under this order; and (2) is not otherwise revealed in the individual items of information. As used in this order, "compilation" means an aggregation of pre-existing unclassified items of information.

Sec. 1.8. Classification Challenges. (a) Authorized holders of information who, in good faith, believe that its classification status is improper are encouraged and expected to challenge the classification status of the information in accordance with agency procedures established under paragraph (b) of this section.

(b) In accordance with implementing directives issued pursuant to this order, an agency head or senior agency official shall establish procedures under which authorized holders of information are encouraged and expected to challenge the classification of information that they believe is improperly classified or unclassified. These procedures shall ensure that:

- (1) individuals are not subject to retribution for bringing such actions;
- (2) an opportunity is provided for review by an impartial official or panel; and
- (3) individuals are advised of their right to appeal agency decisions to the Interagency Security Classification Appeals Panel (Panel) established by section 5.3 of this order.

Part 2—Derivative Classification

Sec. 2.1. Use of Derivative Classification.

(a) Persons who only reproduce, extract, or summarize classified information, or who only apply classification markings derived from source material or as directed by a classification guide, need not possess original classification authority.

(b) Persons who apply derivative classification markings shall:

- (1) observe and respect original classification decisions; and
- (2) carry forward to any newly created documents the pertinent classification markings. For information derivatively classified based on multiple

sources, the derivative classifier shall carry forward:

- (A) the date or event for declassification that corresponds to the longest period of classification among the sources; and
- (B) a listing of these sources on or attached to the official file or record copy.

Sec. 2.2. Classification Guides. (a) Agencies with original classification authority shall prepare classification guides to facilitate the proper and uniform derivative classification of information. These guides shall conform to standards contained in directives issued under this order.

(b) Each guide shall be approved personally and in writing by an official who:

- (1) has program or supervisory responsibility over the information or is the senior agency official; and
- (2) is authorized to classify information originally at the highest level of classification prescribed in the guide.

(c) Agencies shall establish procedures to ensure that classification guides are reviewed and updated as provided in directives issued under this order.

Part 3—Declassification and Downgrading

Sec. 3.1. Authority for Declassification.

(a) Information shall be declassified as soon as it no longer meets the standards for classification under this order.

(b) It is presumed that information that continues to meet the classification requirements under this order requires continued protection. In some exceptional cases, however, the need to protect such information may be outweighed by the public interest in disclosure of the information, and in these cases the information should be declassified. When such questions arise, they shall be referred to the agency head or the senior agency official. That official will determine, as an exercise of discretion, whether the public interest in disclosure outweighs the damage to the national security that might reasonably be expected from disclosure. This provision does not:

- (1) amplify or modify the substantive criteria or procedures for classification; or
- (2) create any substantive or procedural rights subject to judicial review.

(c) If the Director of the Information Security Oversight Office determines that information is classified in violation of this order, the Director may require the information to be declassified by the agency that originated the classification. Any such decision by the Director may be appealed to the President through the Assistant to the President for National Security Affairs. The information shall remain classified pending a prompt decision on the appeal.

(d) The provisions of this section shall also apply to agencies that, under the terms of this order, do not have original classification authority, but had such authority under predecessor orders.

Sec. 3.2. Transferred Records. (a) In the case of classified records transferred in conjunction with a transfer of functions, and not merely for storage purposes, the receiving agency shall be deemed to be the originating agency for purposes of this order.

(b) In the case of classified records that are not officially transferred as described in paragraph (a) of this section, but that originated in an agency that has ceased to exist and for which there is no successor agency, each agency in possession of such records shall be deemed to be the originating agency for purposes of this order. Such records may be declassified or downgraded by the agency in possession after consultation with any other agency that has an interest in the subject matter of the records.

(c) Classified records accessioned into the National Archives and Records Administration (National Archives) as of the effective date of this order shall be declassified or downgraded by the Archivist of the United States (Archivist) in accordance with this order, the directives issued pursuant to this order, agency declassification guides, and any existing procedural agreement between the Archivist and the relevant agency head.

(d) The originating agency shall take all reasonable steps to declassify classified information contained in records determined to have permanent historical value before they

are accessioned into the National Archives. However, the Archivist may require that classified records be accessioned into the National Archives when necessary to comply with the provisions of the Federal Records Act. This provision does not apply to records being transferred to the Archivist pursuant to section 2203 of title 44, United States Code, or records for which the National Archives serves as the custodian of the records of an agency or organization that has gone out of existence.

(e) To the extent practicable, agencies shall adopt a system of records management that will facilitate the public release of documents at the time such documents are declassified pursuant to the provisions for automatic declassification in section 3.3 of this order.

Sec. 3.3. Automatic Declassification. (a) Subject to paragraphs (b)–(e) of this section, on December 31, 2006, all classified records that (1) are more than 25 years old and (2) have been determined to have permanent historical value under title 44, United States Code, shall be automatically declassified whether or not the records have been reviewed. Subsequently, all classified records shall be automatically declassified on December 31 of the year that is 25 years from the date of its original classification, except as provided in paragraphs (b)–(e) of this section.

(b) An agency head may exempt from automatic declassification under paragraph (a) of this section specific information, the release of which could be expected to:

- (1) reveal the identity of a confidential human source, or a human intelligence source, or reveal information about the application of an intelligence source or method;
- (2) reveal information that would assist in the development or use of weapons of mass destruction;
- (3) reveal information that would impair U.S. cryptologic systems or activities;
- (4) reveal information that would impair the application of state of the art technology within a U.S. weapon system;
- (5) reveal actual U.S. military war plans that remain in effect;

- (6) reveal information, including foreign government information, that would seriously and demonstrably impair relations between the United States and a foreign government, or seriously and demonstrably undermine ongoing diplomatic activities of the United States;
- (7) reveal information that would clearly and demonstrably impair the current ability of United States Government officials to protect the President, Vice President, and other protectees for whom protection services, in the interest of the national security, are authorized;
- (8) reveal information that would seriously and demonstrably impair current national security emergency preparedness plans or reveal current vulnerabilities of systems, installations, infrastructures, or projects relating to the national security; or
- (9) violate a statute, treaty, or international agreement.

(c) An agency head shall notify the President through the Assistant to the President for National Security Affairs of any specific file series of records for which a review or assessment has determined that the information within that file series almost invariably falls within one or more of the exemption categories listed in paragraph (b) of this section and which the agency proposes to exempt from automatic declassification. The notification shall include:

- (1) a description of the file series;
- (2) an explanation of why the information within the file series is almost invariably exempt from automatic declassification and why the information must remain classified for a longer period of time; and
- (3) except for the identity of a confidential human source or a human intelligence source, as provided in paragraph (b) of this section, a specific date or event for declassification of the information.

The President may direct the agency head not to exempt the file series or to declassify the information within that series at an earlier date than recommended. File series ex-

emptions previously approved by the President shall remain valid without any additional agency action.

(d) At least 180 days before information is automatically declassified under this section, an agency head or senior agency official shall notify the Director of the Information Security Oversight Office, serving as Executive Secretary of the Panel, of any specific information beyond that included in a notification to the President under paragraph (c) of this section that the agency proposes to exempt from automatic declassification. The notification shall include:

- (1) a description of the information, either by reference to information in specific records or in the form of a declassification guide;
- (2) an explanation of why the information is exempt from automatic declassification and must remain classified for a longer period of time; and
- (3) except for the identity of a confidential human source or a human intelligence source, as provided in paragraph (b) of this section, a specific date or event for declassification of the information. The Panel may direct the agency not to exempt the information or to declassify it at an earlier date than recommended. The agency head may appeal such a decision to the President through the Assistant to the President for National Security Affairs. The information will remain classified while such an appeal is pending.

(e) The following provisions shall apply to the onset of automatic declassification:

- (1) Classified records within an integral file block, as defined in this order, that are otherwise subject to automatic declassification under this section shall not be automatically declassified until December 31 of the year that is 25 years from the date of the most recent record within the file block.
- (2) By notification to the Director of the Information Security Oversight Office, before the records are subject to automatic declassification, an agency

head or senior agency official designated under section 5.4 of this order may delay automatic declassification for up to 5 additional years for classified information contained in microforms, motion pictures, audiotapes, videotapes, or comparable media that make a review for possible declassification exemptions more difficult or costly.

- (3) By notification to the Director of the Information Security Oversight Office, before the records are subject to automatic declassification, an agency head or senior agency official designated under section 5.4 of this order may delay automatic declassification for up to 3 years for classified records that have been referred or transferred to that agency by another agency less than 3 years before automatic declassification would otherwise be required.
- (4) By notification to the Director of the Information Security Oversight Office, an agency head or senior agency official designated under section 5.4 of this order may delay automatic declassification for up to 3 years from the date of discovery of classified records that were inadvertently not reviewed prior to the effective date of automatic declassification.
- (f) Information exempted from automatic declassification under this section shall remain subject to the mandatory and systematic declassification review provisions of this order.
- (g) The Secretary of State shall determine when the United States should commence negotiations with the appropriate officials of a foreign government or international organization of governments to modify any treaty or international agreement that requires the classification of information contained in records affected by this section for a period longer than 25 years from the date of its creation, unless the treaty or international agreement pertains to information that may otherwise remain classified beyond 25 years under this section.
- (h) Records containing information that originated with other agencies or the disclo-

sure of which would affect the interests or activities of other agencies shall be referred for review to those agencies and the information of concern shall be subject to automatic declassification only by those agencies, consistent with the provisions of subparagraphs (e)(3) and (e)(4) of this section.

Sec. 3.4. Systematic Declassification Review. (a) Each agency that has originated classified information under this order or its predecessors shall establish and conduct a program for systematic declassification review. This program shall apply to records of permanent historical value exempted from automatic declassification under section 3.3 of this order. Agencies shall prioritize the systematic review of records based upon the degree of researcher interest and the likelihood of declassification upon review.

(b) The Archivist shall conduct a systematic declassification review program for classified records: (1) accessioned into the National Archives as of the effective date of this order; (2) transferred to the Archivist pursuant to section 2203 of title 44, United States Code; and (3) for which the National Archives serves as the custodian for an agency or organization that has gone out of existence. This program shall apply to pertinent records no later than 25 years from the date of their creation. The Archivist shall establish priorities for the systematic review of these records based upon the degree of researcher interest and the likelihood of declassification upon review. These records shall be reviewed in accordance with the standards of this order, its implementing directives, and declassification guides provided to the Archivist by each agency that originated the records. The Director of the Information Security Oversight Office shall ensure that agencies provide the Archivist with adequate and current declassification guides.

(c) After consultation with affected agencies, the Secretary of Defense may establish special procedures for systematic review for declassification of classified cryptologic information, and the Director of Central Intelligence may establish special procedures for systematic review for declassification of classified information pertaining to intelligence activities (including special activities), or intelligence sources or methods.

Sec. 3.5. Mandatory Declassification Review. (a) Except as provided in paragraph (b) of this section, all information classified under this order or predecessor orders shall be subject to a review for declassification by the originating agency if:

- (1) the request for a review describes the document or material containing the information with sufficient specificity to enable the agency to locate it with a reasonable amount of effort;
- (2) the information is not exempted from search and review under sections 105C, 105D, or 701 of the National Security Act of 1947 (50 U.S.C. 403-5c, 403-5e, and 431); and
- (3) the information has not been reviewed for declassification within the past 2 years. If the agency has reviewed the information within the past 2 years, or the information is the subject of pending litigation, the agency shall inform the requester of this fact and of the requester's appeal rights.

(b) Information originated by:

- (1) the incumbent President or, in the performance of executive duties, the incumbent Vice President;
- (2) the incumbent President's White House Staff or, in the performance of executive duties, the incumbent Vice President's Staff;
- (3) committees, commissions, or boards appointed by the incumbent President; or
- (4) other entities within the Executive Office of the President that solely advise and assist the incumbent President is exempted from the provisions of paragraph (a) of this section. However, the Archivist shall have the authority to review, downgrade, and declassify papers or records of former Presidents under the control of the Archivist pursuant to sections 2107, 2111, 2111 note, or 2203 of title 44, United States Code. Review procedures developed by the Archivist shall provide for consultation with agencies having primary subject matter interest and shall be consistent with the provisions of applicable laws or lawful

agreements that pertain to the respective Presidential papers or records. Agencies with primary subject matter interest shall be notified promptly of the Archivist's decision. Any final decision by the Archivist may be appealed by the requester or an agency to the Panel. The information shall remain classified pending a prompt decision on the appeal.

(c) Agencies conducting a mandatory review for declassification shall declassify information that no longer meets the standards for classification under this order. They shall release this information unless withholding is otherwise authorized and warranted under applicable law.

(d) In accordance with directives issued pursuant to this order, agency heads shall develop procedures to process requests for the mandatory review of classified information. These procedures shall apply to information classified under this or predecessor orders. They also shall provide a means for administratively appealing a denial of a mandatory review request, and for notifying the requester of the right to appeal a final agency decision to the Panel.

(e) After consultation with affected agencies, the Secretary of Defense shall develop special procedures for the review of cryptologic information; the Director of Central Intelligence shall develop special procedures for the review of information pertaining to intelligence activities (including special activities), or intelligence sources or methods; and the Archivist shall develop special procedures for the review of information accessioned into the National Archives.

Sec. 3.6. Processing Requests and Reviews. In response to a request for information under the Freedom of Information Act, the Privacy Act of 1974, or the mandatory review provisions of this order, or pursuant to the automatic declassification or systematic review provisions of this order:

(a) An agency may refuse to confirm or deny the existence or nonexistence of requested records whenever the fact of their existence or nonexistence is itself classified under this order or its predecessors.

(b) When an agency receives any request for documents in its custody that contain information that was originally classified by another agency, or comes across such documents in the process of the automatic declassification or systematic review provisions of this order, it shall refer copies of any request and the pertinent documents to the originating agency for processing, and may, after consultation with the originating agency, inform any requester of the referral unless such association is itself classified under this order or its predecessors. In cases in which the originating agency determines in writing that a response under paragraph (a) of this section is required, the referring agency shall respond to the requester in accordance with that paragraph.

Sec. 3.7. Declassification Database. (a) The Director of the Information Security Oversight Office, in conjunction with those agencies that originate classified information, shall coordinate the linkage and effective utilization of existing agency databases of records that have been declassified and publicly released.

(b) Agency heads shall fully cooperate with the Director of the Information Security Oversight Office in these efforts.

Part 4—Safeguarding

Sec. 4.1. General Restrictions on Access.

(a) A person may have access to classified information provided that:

- (1) a favorable determination of eligibility for access has been made by an agency head or the agency head's designee;
- (2) the person has signed an approved nondisclosure agreement; and
- (3) the person has a need-to-know the information.

(b) Every person who has met the standards for access to classified information in paragraph (a) of this section shall receive contemporaneous training on the proper safeguarding of classified information and on the criminal, civil, and administrative sanctions that may be imposed on an individual who fails to protect classified information from unauthorized disclosure.

(c) Classified information shall remain under the control of the originating agency

or its successor in function. An agency shall not disclose information originally classified by another agency without its authorization. An official or employee leaving agency service may not remove classified information from the agency's control.

(d) Classified information may not be removed from official premises without proper authorization.

(e) Persons authorized to disseminate classified information outside the executive branch shall ensure the protection of the information in a manner equivalent to that provided within the executive branch.

(f) Consistent with law, directives, and regulation, an agency head or senior agency official shall establish uniform procedures to ensure that automated information systems, including networks and telecommunications systems, that collect, create, communicate, compute, disseminate, process, or store classified information have controls that:

- (1) prevent access by unauthorized persons; and
- (2) ensure the integrity of the information.

(g) Consistent with law, directives, and regulation, each agency head or senior agency official shall establish controls to ensure that classified information is used, processed, stored, reproduced, transmitted, and destroyed under conditions that provide adequate protection and prevent access by unauthorized persons.

(h) Consistent with directives issued pursuant to this order, an agency shall safeguard foreign government information under standards that provide a degree of protection at least equivalent to that required by the government or international organization of governments that furnished the information. When adequate to achieve equivalency, these standards may be less restrictive than the safeguarding standards that ordinarily apply to United States "Confidential" information, including modified handling and transmission and allowing access to individuals with a need-to-know who have not otherwise been cleared for access to classified information or executed an approved nondisclosure agreement.

(i) Except as otherwise provided by statute, this order, directives implementing this

order, or by direction of the President, classified information originating in one agency shall not be disseminated outside any other agency to which it has been made available without the consent of the originating agency. An agency head or senior agency official may waive this requirement for specific information originated within that agency. For purposes of this section, the Department of Defense shall be considered one agency. Prior consent is not required when referring records for declassification review that contain information originating in several agencies.

Sec. 4.2. Distribution Controls. (a) Each agency shall establish controls over the distribution of classified information to ensure that it is distributed only to organizations or individuals eligible for access and with a need-to-know the information.

(b) In an emergency, when necessary to respond to an imminent threat to life or in defense of the homeland, the agency head or any designee may authorize the disclosure of classified information to an individual or individuals who are otherwise not eligible for access. Such actions shall be taken only in accordance with the directives implementing this order and any procedures issued by agencies governing the classified information, which shall be designed to minimize the classified information that is disclosed under these circumstances and the number of individuals who receive it. Information disclosed under this provision or implementing directives and procedures shall not be deemed declassified as a result of such disclosure or subsequent use by a recipient. Such disclosures shall be reported promptly to the originator of the classified information. For purposes of this section, the Director of Central Intelligence may issue an implementing directive governing the emergency disclosure of classified intelligence information.

(c) Each agency shall update, at least annually, the automatic, routine, or recurring distribution of classified information that they distribute. Recipients shall cooperate fully with distributors who are updating distribution lists and shall notify distributors whenever a relevant change in status occurs.

Sec. 4.3. Special Access Programs. (a) Establishment of special access programs. Un-

less otherwise authorized by the President, only the Secretaries of State, Defense, and Energy, and the Director of Central Intelligence, or the principal deputy of each, may create a special access program. For special access programs pertaining to intelligence activities (including special activities, but not including military operational, strategic, and tactical programs), or intelligence sources or methods, this function shall be exercised by the Director of Central Intelligence. These officials shall keep the number of these programs at an absolute minimum, and shall establish them only when the program is required by statute or upon a specific finding that:

- (1) the vulnerability of, or threat to, specific information is exceptional; and
- (2) the normal criteria for determining eligibility for access applicable to information classified at the same level are not deemed sufficient to protect the information from unauthorized disclosure.

(b) Requirements and limitations. (1) Special access programs shall be limited to programs in which the number of persons who will have access ordinarily will be reasonably small and commensurate with the objective of providing enhanced protection for the information involved.

- (2) Each agency head shall establish and maintain a system of accounting for special access programs consistent with directives issued pursuant to this order.

- (3) Special access programs shall be subject to the oversight program established under section 5.4(d) of this order. In addition, the Director of the Information Security Oversight Office shall be afforded access to these programs, in accordance with the security requirements of each program, in order to perform the functions assigned to the Information Security Oversight Office under this order. An agency head may limit access to a special access program to the Director and no more than one other employee of the Information Security Oversight Office, or, for special access programs

that are extraordinarily sensitive and vulnerable, to the Director only.

- (4) The agency head or principal deputy shall review annually each special access program to determine whether it continues to meet the requirements of this order.
- (5) Upon request, an agency head shall brief the Assistant to the President for National Security Affairs, or a designee, on any or all of the agency's special access programs.
- (c) Nothing in this order shall supersede any requirement made by or under 10 U.S.C. 119.

Sec. 4.4. Access by Historical Researchers and Certain Former Government Personnel. (a) The requirement in section 4.1(a)(3) of this order that access to classified information may be granted only to individuals who have a need-to-know the information may be waived for persons who:

- (1) are engaged in historical research projects;
- (2) previously have occupied policy-making positions to which they were appointed by the President under section 105(a)(2)(A) of title 3, United States Code, or the Vice President under 106(a)(1)(A) of title 3, United States Code; or
- (3) served as President or Vice President.
- (b) Waivers under this section may be granted only if the agency head or senior agency official of the originating agency:

 - (1) determines in writing that access is consistent with the interest of the national security;
 - (2) takes appropriate steps to protect classified information from unauthorized disclosure or compromise, and ensures that the information is safeguarded in a manner consistent with this order; and
 - (3) limits the access granted to former Presidential appointees and Vice Presidential appointees to items that the person originated, reviewed, signed, or received while serving as

a Presidential appointee or a Vice Presidential appointee.

Part 5—Implementation and Review

Sec. 5.1. Program Direction. (a) The Director of the Information Security Oversight Office, under the direction of the Archivist and in consultation with the Assistant to the President for National Security Affairs, shall issue such directives as are necessary to implement this order. These directives shall be binding upon the agencies. Directives issued by the Director of the Information Security Oversight Office shall establish standards for:

- (1) classification and marking principles;
- (2) safeguarding classified information, which shall pertain to the handling, storage, distribution, transmittal, and destruction of and accounting for classified information;
- (3) agency security education and training programs;
- (4) agency self-inspection programs; and
- (5) classification and declassification guides.

(b) The Archivist shall delegate the implementation and monitoring functions of this program to the Director of the Information Security Oversight Office.

Sec. 5.2. Information Security Oversight Office. (a) There is established within the National Archives an Information Security Oversight Office. The Archivist shall appoint the Director of the Information Security Oversight Office, subject to the approval of the President.

(b) Under the direction of the Archivist, acting in consultation with the Assistant to the President for National Security Affairs, the Director of the Information Security Oversight Office shall:

- (1) develop directives for the implementation of this order;
- (2) oversee agency actions to ensure compliance with this order and its implementing directives;
- (3) review and approve agency implementing regulations and agency guides for systematic declassification

review prior to their issuance by the agency;

(4) have the authority to conduct on-site reviews of each agency's program established under this order, and to require of each agency those reports, information, and other cooperation that may be necessary to fulfill its responsibilities. If granting access to specific categories of classified information would pose an exceptional national security risk, the affected agency head or the senior agency official shall submit a written justification recommending the denial of access to the President through the Assistant to the President for National Security Affairs within 60 days of the request for access. Access shall be denied pending the response;

(5) review requests for original classification authority from agencies or officials not granted original classification authority and, if deemed appropriate, recommend Presidential approval through the Assistant to the President for National Security Affairs;

(6) consider and take action on complaints and suggestions from persons within or outside the Government with respect to the administration of the program established under this order;

(7) have the authority to prescribe, after consultation with affected agencies, standardization of forms or procedures that will promote the implementation of the program established under this order;

(8) report at least annually to the President on the implementation of this order; and

(9) convene and chair interagency meetings to discuss matters pertaining to the program established by this order.

Sec. 5.3. Interagency Security Classification Appeals Panel.

(a) Establishment and administration.

(1) There is established an Interagency Security Classification Appeals Panel. The Departments of State, Defense, and Justice, the Central Intelligence Agency, the National Archives, and the Assistant to the President for National Security Affairs shall each be represented by a senior-level representative who is a full-time or permanent part-time Federal officer or employee designated to serve as a member of the Panel by the respective agency head. The President shall select the Chair of the Panel from among the Panel members.

(2) A vacancy on the Panel shall be filled as quickly as possible as provided in paragraph (a)(1) of this section.

(3) The Director of the Information Security Oversight Office shall serve as the Executive Secretary. The staff of the Information Security Oversight Office shall provide program and administrative support for the Panel.

(4) The members and staff of the Panel shall be required to meet eligibility for access standards in order to fulfill the Panel's functions.

(5) The Panel shall meet at the call of the Chair. The Chair shall schedule meetings as may be necessary for the Panel to fulfill its functions in a timely manner.

(6) The Information Security Oversight Office shall include in its reports to the President a summary of the Panel's activities.

(b) Functions. The Panel shall:

(1) decide on appeals by persons who have filed classification challenges under section 1.8 of this order;

(2) approve, deny, or amend agency exemptions from automatic declassification as provided in section 3.3 of this order; and

(3) decide on appeals by persons or entities who have filed requests for mandatory declassification review under section 3.5 of this order.

(c) Rules and procedures. The Panel shall issue bylaws, which shall be published in the *Federal Register*. The bylaws shall establish the rules and procedures that the Panel will follow in accepting, considering, and issuing decisions on appeals. The rules and procedures of the Panel shall provide that the Panel will consider appeals only on actions in which:

- (1) the appellant has exhausted his or her administrative remedies within the responsible agency;
- (2) there is no current action pending on the issue within the Federal courts; and
- (3) the information has not been the subject of review by the Federal courts or the Panel within the past 2 years.
- (d) Agency heads shall cooperate fully with the Panel so that it can fulfill its functions in a timely and fully informed manner. An agency head may appeal a decision of the Panel to the President through the Assistant to the President for National Security Affairs. The Panel shall report to the President through the Assistant to the President for National Security Affairs any instance in which it believes that an agency head is not cooperating fully with the Panel.
- (e) The Panel is established for the sole purpose of advising and assisting the President in the discharge of his constitutional and discretionary authority to protect the national security of the United States. Panel decisions are committed to the discretion of the Panel, unless changed by the President.
- (f) Notwithstanding paragraphs (a) through (e) of this section, whenever the Panel reaches a conclusion that information owned or controlled by the Director of Central Intelligence (Director) should be declassified, and the Director notifies the Panel that he objects to its conclusion because he has determined that the information could reasonably be expected to cause damage to the national security and to reveal (1) the identity of a human intelligence source, or (2) information about the application of an intelligence source or method (including any information that concerns, or is provided as a result of, a relationship with a cooperating intelligence element of a foreign government), the information shall remain classified unless the Director's determination is appealed to the President, and the President reverses the determination.

Sec. 5.4. General Responsibilities. Heads of agencies that originate or handle classified information shall:

- (a) demonstrate personal commitment and commit senior management to the successful implementation of the program established under this order;
- (b) commit necessary resources to the effective implementation of the program established under this order;
- (c) ensure that agency records systems are designed and maintained to optimize the safeguarding of classified information, and to facilitate its declassification under the terms of this order when it no longer meets the standards for continued classification; and
- (d) designate a senior agency official to direct and administer the program, whose responsibilities shall include:
 - (1) overseeing the agency's program established under this order, provided, an agency head may designate a separate official to oversee special access programs authorized under this order. This official shall provide a full accounting of the agency's special access programs at least annually;
 - (2) promulgating implementing regulations, which shall be published in the *Federal Register* to the extent that they affect members of the public;
 - (3) establishing and maintaining security education and training programs;
 - (4) establishing and maintaining an ongoing self-inspection program, which shall include the periodic review and assessment of the agency's classified product;
 - (5) establishing procedures to prevent unnecessary access to classified information, including procedures that:
 - (A) require that a need for access to classified information is established before initiating administrative clearance procedures; and
 - (B) ensure that the number of persons granted access to classified information is limited to the minimum consistent with operational and security requirements and needs;
 - (6) developing special contingency plans for the safeguarding of classified information used in or near hostile or potentially hostile areas;
 - (7) ensuring that the performance contract or other system used to rate civilian or military personnel performance includes the management of

classified information as a critical element or item to be evaluated in the rating of:

- (A) original classification authorities;
- (B) security managers or security specialists; and
- (C) all other personnel whose duties significantly involve the creation or handling of classified information;
- (8) accounting for the costs associated with the implementation of this order, which shall be reported to the Director of the Information Security Oversight Office for publication; and
- (9) assigning in a prompt manner agency personnel to respond to any request, appeal, challenge, complaint, or suggestion arising out of this order that pertains to classified information that originated in a component of the agency that no longer exists and for which there is no clear successor in function.

Sec. 5.5. Sanctions. (a) If the Director of the Information Security Oversight Office finds that a violation of this order or its implementing directives has occurred, the Director shall make a report to the head of the agency or to the senior agency official so that corrective steps, if appropriate, may be taken.

(b) Officers and employees of the United States Government, and its contractors, licensees, certificate holders, and grantees shall be subject to appropriate sanctions if they knowingly, willfully, or negligently:

- (1) disclose to unauthorized persons information properly classified under this order or predecessor orders;
- (2) classify or continue the classification of information in violation of this order or any implementing directive;
- (3) create or continue a special access program contrary to the requirements of this order; or
- (4) contravene any other provision of this order or its implementing directives.

(c) Sanctions may include reprimand, suspension without pay, removal, termination of classification authority, loss or denial of access to classified information, or other sanctions in accordance with applicable law and agency regulation.

(d) The agency head, senior agency official, or other supervisory official shall, at a minimum, promptly remove the classification authority of any individual who demonstrates reckless disregard or a pattern of error in applying the classification standards of this order.

(e) The agency head or senior agency official shall:

- (1) take appropriate and prompt corrective action when a violation or infraction under paragraph (b) of this section occurs; and
- (2) notify the Director of the Information Security Oversight Office when a violation under paragraph (b)(1), (2), or (3) of this section occurs.

Part 6—General Provisions

Sec. 6.1. Definitions. For purposes of this order:

(a) “Access” means the ability or opportunity to gain knowledge of classified information.

(b) “Agency” means any “Executive agency,” as defined in 5 U.S.C. 105; any “Military department” as defined in 5 U.S.C. 102; and any other entity within the executive branch that comes into the possession of classified information.

(c) “Automated information system” means an assembly of computer hardware, software, or firmware configured to collect, create, communicate, compute, disseminate, process, store, or control data or information.

(d) “Automatic declassification” means the declassification of information based solely upon:

- (1) the occurrence of a specific date or event as determined by the original classification authority; or
- (2) the expiration of a maximum time frame for duration of classification established under this order.

(e) “Classification” means the act or process by which information is determined to be classified information.

(f) “Classification guidance” means any instruction or source that prescribes the classification of specific information.

(g) “Classification guide” means a documentary form of classification guidance issued by an original classification authority

that identifies the elements of information regarding a specific subject that must be classified and establishes the level and duration of classification for each such element.

(h) "Classified national security information" or "classified information" means information that has been determined pursuant to this order or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

(i) "Confidential source" means any individual or organization that has provided, or that may reasonably be expected to provide, information to the United States on matters pertaining to the national security with the expectation that the information or relationship, or both, are to be held in confidence.

(j) "Damage to the national security" means harm to the national defense or foreign relations of the United States from the unauthorized disclosure of information, taking into consideration such aspects of the information as the sensitivity, value, utility, and provenance of that information.

(k) "Declassification" means the authorized change in the status of information from classified information to unclassified information.

(l) "Declassification authority" means:

- (1) the official who authorized the original classification, if that official is still serving in the same position;
- (2) the originator's current successor in function;
- (3) a supervisory official of either; or
- (4) officials delegated declassification authority in writing by the agency head or the senior agency official.

(m) "Declassification guide" means written instructions issued by a declassification authority that describes the elements of information regarding a specific subject that may be declassified and the elements that must remain classified.

(n) "Derivative classification" means the incorporating, paraphrasing, restating, or generating in new form information that is already classified, and marking the newly developed material consistent with the classification markings that apply to the source information. Derivative classification includes the classification of information based on

classification guidance. The duplication or reproduction of existing classified information is not derivative classification.

(o) "Document" means any recorded information, regardless of the nature of the medium or the method or circumstances of recording.

(p) "Downgrading" means a determination by a declassification authority that information classified and safeguarded at a specified level shall be classified and safeguarded at a lower level.

(q) "File series" means file units or documents arranged according to a filing system or kept together because they relate to a particular subject or function, result from the same activity, document a specific kind of transaction, take a particular physical form, or have some other relationship arising out of their creation, receipt, or use, such as restrictions on access or use.

(r) "Foreign government information" means:

- (1) information provided to the United States Government by a foreign government or governments, an international organization of governments, or any element thereof, with the expectation that the information, the source of the information, or both, are to be held in confidence;
- (2) information produced by the United States Government pursuant to or as a result of a joint arrangement with a foreign government or governments, or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence; or
- (3) information received and treated as "foreign government information" under the terms of a predecessor order.

(s) "Information" means any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics, that is owned by, produced by or for, or is under the control of the United States Government. "Control" means the authority of the agency that originates information, or its successor in function, to regulate access to the information.

(t) "Infraction" means any knowing, willful, or negligent action contrary to the requirements of this order or its implementing directives that does not constitute a "violation," as defined below.

(u) "Integral file block" means a distinct component of a file series, as defined in this section, that should be maintained as a separate unit in order to ensure the integrity of the records. An integral file block may consist of a set of records covering either a specific topic or a range of time such as presidential administration or a 5-year retirement schedule within a specific file series that is retired from active use as a group.

(v) "Integrity" means the state that exists when information is unchanged from its source and has not been accidentally or intentionally modified, altered, or destroyed.

(w) "Mandatory declassification review" means the review for declassification of classified information in response to a request for declassification that meets the requirements under section 3.5 of this order.

(x) "Multiple sources" means two or more source documents, classification guides, or a combination of both.

(y) "National security" means the national defense or foreign relations of the United States.

(z) "Need-to-know" means a determination made by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.

(aa) "Network" means a system of two or more computers that can exchange data or information.

(bb) "Original classification" means an initial determination that information requires, in the interest of the national security, protection against unauthorized disclosure.

(cc) "Original classification authority" means an individual authorized in writing, either by the President, the Vice President in the performance of executive duties, or by agency heads or other officials designated by the President, to classify information in the first instance.

(dd) "Records" means the records of an agency and Presidential papers or Presidential records, as those terms are defined

in title 44, United States Code, including those created or maintained by a government contractor, licensee, certificate holder, or grantee that are subject to the sponsoring agency's control under the terms of the contract, license, certificate, or grant.

(ee) "Records having permanent historical value" means Presidential papers or Presidential records and the records of an agency that the Archivist has determined should be maintained permanently in accordance with title 44, United States Code.

(ff) "Records management" means the planning, controlling, directing, organizing, training, promoting, and other managerial activities involved with respect to records creation, records maintenance and use, and records disposition in order to achieve adequate and proper documentation of the policies and transactions of the Federal Government and effective and economical management of agency operations.

(gg) "Safeguarding" means measures and controls that are prescribed to protect classified information.

(hh) "Self-inspection" means the internal review and evaluation of individual agency activities and the agency as a whole with respect to the implementation of the program established under this order and its implementing directives.

(ii) "Senior agency official" means the official designated by the agency head under section 5.4(d) of this order to direct and administer the agency's program under which information is classified, safeguarded, and declassified.

(jj) "Source document" means an existing document that contains classified information that is incorporated, paraphrased, restated, or generated in new form into a new document.

(kk) "Special access program" means a program established for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level.

(ll) "Systematic declassification review" means the review for declassification of classified information contained in records that have been determined by the Archivist to

have permanent historical value in accordance with title 44, United States Code.

(mm) "Telecommunications" means the preparation, transmission, or communication of information by electronic means.

(nn) "Unauthorized disclosure" means a communication or physical transfer of classified information to an unauthorized recipient.

(oo) "Violation" means:

- (1) any knowing, willful, or negligent action that could reasonably be expected to result in an unauthorized disclosure of classified information;
- (2) any knowing, willful, or negligent action to classify or continue the classification of information contrary to the requirements of this order or its implementing directives; or
- (3) any knowing, willful, or negligent action to create or continue a special access program contrary to the requirements of this order.

(pp) "Weapons of mass destruction" means chemical, biological, radiological, and nuclear weapons.

Sec. 6.2. General Provisions. (a) Nothing in this order shall supersede any requirement made by or under the Atomic Energy Act of 1954, as amended, or the National Security Act of 1947, as amended. "Restricted Data" and "Formerly Restricted Data" shall be handled, protected, classified, downgraded, and declassified in conformity with the provisions of the Atomic Energy Act of 1954, as amended, and regulations issued under that Act.

(b) The Attorney General, upon request by the head of an agency or the Director of the Information Security Oversight Office, shall render an interpretation of this order with respect to any question arising in the course of its administration.

(c) Nothing in this order limits the protection afforded any information by other provisions of law, including the Constitution, Freedom of Information Act exemptions, the Privacy Act of 1974, and the National Security Act of 1947, as amended. This order is not intended to and does not create any right or benefit, substantive or procedural, enforceable at law by a party against the United States, its departments, agencies, officers,

employees, or agents. The foregoing is in addition to the specific provisos set forth in sections 3.1(b) and 5.3(e) of this order."

(d) Executive Order 12356 of April 6, 1982, was revoked as of October 14, 1995.

Sec. 6.3. Effective Date. This order is effective immediately, except for section 1.6, which shall become effective 180 days from the date of this order.

George W. Bush

The White House,
March 25, 2003.

[Filed with the Office of the Federal Register, 9:17 a.m., March 27, 2003]

NOTE: This Executive order was published in the *Federal Register* on March 28.

Letter to the Speaker of the House of Representatives Transmitting a Supplemental Budget Request To Support Military and Humanitarian Operations in Iraq and To Ensure Domestic Safety

March 25, 2003

Dear Mr. Speaker:

On October 16, 2002, I signed into law the "Authorization for Use of Military Force Against Iraq Resolution of 2002" (Public Law 107-243). After condemning Saddam Hussein's continued possession of chemical and biological weapons, obstruction of inspections, and brutal repression of the Iraqi people, the Congress affirmed, "Iraq poses a continuing threat to the national security of the United States and international peace and security of the Persian Gulf region and remains in material and unacceptable breach of its international obligations."

Subsequent to enactment of Public Law 107-243, the United Nations Security Council unanimously agreed to Resolution 1441 offering Iraq one final chance to disarm. After more than a decade of deceit and defiance, the regime, yet again, failed to "fully and unconditionally" comply. Iraq continues to pose a grave danger to global peace and security. The United States and our allies must seek to disarm Iraq and liberate the Iraqi people, and we will prevail.