DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
----------	)	ISCR Case No. 11-07728
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Julie R. Mendez, Esq., Department Counsel
For Applicant: Mark S. Zaid, Esq.

01/21/2016

Decision

HARVEY, Mark, Administrative Judge:

Applicant's statement of reasons (SOR) alleges two allegations under Guideline K (handling protected information) and five allegations under Guideline E (personal conduct). All allegations relate to his handling of confidential data in December 2007 and January 2008 and his participation in the follow-up investigation in 2009 and 2010. Applicant was assured that "trusted downloads" provided by the Navy and Company L did not contain classified information, when two of them contained a mix of unclassified and classified information. Applicant and his team members transferred the trusted downloads onto computers that were for unclassified use only. There was no evidence that any of the classified information was viewed by anyone not authorized to view it. Applicant made some judgment errors in his reaction to the discovery of the classified information. In March 2008, Applicant's attorney offered to provide requested materials to the Federal Bureau of Investigation (FBI); Applicant cooperated with the investigation; and Applicant's errors in judgment are not recent. He credibly assured conscientious compliance with security rules. He presented a strong case of whole-person mitigation. Security concerns are mitigated. Access to classified information is granted.

History of the Case

On February 11, 2011, Applicant completed and signed an Electronic Questionnaires for Investigations Processing (e-QIP) (SF 86). (Government Exhibit (GE) 1) On August 18, 2014, the Department of Defense (DOD) Consolidated Adjudications Facility (CAF) issued an SOR to Applicant pursuant to Executive Order

(Exec. Or.) 10865, *Safeguarding Classified Information Within Industry,* dated February 20, 1960, as amended; DOD Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (Directive), dated January 2, 1992, as amended; and the adjudicative guidelines (AG), which became effective on September 1, 2006.

The SOR detailed reasons why the DOD CAF could not make the affirmative finding under the Directive that it is clearly consistent with the national interest to grant or continue a security clearance for Applicant and recommended referral to an administrative judge to determine whether a clearance should be granted, continued, denied, or revoked. (Hearing Exhibit (HE) 2) Specifically, the SOR set forth security concerns arising under Guidelines K and E.

On September 2, 2014, Applicant responded to the SOR, and he requested a hearing. On July 23, 2015, Department Counsel was ready to proceed. On July 30, 2015, the case was assigned to me. On November 12, 2015, the Defense Office of Hearings and Appeals (DOHA) issued a notice of hearing, setting the hearing for December 14, 2015. (HE 1) The hearing was held as scheduled. On December 7, 2015, Department Counsel moved to amend the allegation in SOR ¶ 1.b. There was no objection, and I granted the motion. During the hearing, Department Counsel offered seven exhibits, which were admitted into evidence without objection, and Applicant offered 18 exhibits, which were admitted without objection. (Transcript (Tr.) 17-21; Government Exhibit (GE) 1-7; Applicant Exhibit (AE) A-R) On December 22, 2015, I received a transcript of the hearing.

Findings of Fact

In Applicant's SOR response, he denied all of the SOR allegations. Applicant admitted the information in amended SOR ¶ 1.b. Applicant's admissions are accepted as findings of fact.

Applicant is a 56-year-old software engineer employed by Company D, a defense contractor from 1980 to 2007. (Tr. 179, 214; AE A) From 2008 to present, he has been employed by another defense contractor. (AE A) In January 2011, Applicant's security clearance was suspended. (GE 2; AE E)

In 1998, Applicant married. (Tr. 235) His spouse is a missile engineer, and she has a security clearance. (Tr. 216) He has two daughters who are 14 and 15. (Tr. 215) His father was a career Navy officer. (Tr. 215) His two older brothers served in the Navy. (Tr. 215) His nephew was a Navy Seal, who served three tours in Afghanistan. (Tr. 215) Applicant never served in the military. (Tr. 235)

Company D funded Applicant's college tuition, and in 1982, Applicant received a bachelor of science degree in mathematics. (Tr. 178-179, 235; AE A) After 1982, Applicant worked on a variety of Navy contracts for Company D. Sometimes he was employed at Company D, but detailed to work on Company L managed projects. (Tr. 180) During Desert Shield, he was deployed for six months to the Persian Gulf aboard a U.S. Navy vessel. (Tr. 180)

In 1999, Applicant was one of the architects of a program for a simulation test of part of a weapons system developed by Company L by utilizing unclassified data. (Tr. 184; GE 5; GE 6) From 1999 to 2007, Applicant was instrumental in the program development. (Tr. 184-189). In November 2007, Applicant went to the Pentagon, and in the presence of an admiral, was shown some design charts, which Applicant had developed on behalf of Company D, and Company L had previously presented without authorization to the Navy. (Tr. 189) Applicant believed the information was improperly taken from Company D by Company L.

Handling Protected Information and Personal Conduct[1]

Applicant was the leader of a team of technicians working on a Navy project. (Tr. 99; GE 5 at 1-2) On about 75 occasions over several years, Company L employees or Navy personnel provided "trusted downloads" on flash drives or compact discs, which were supposed to be unclassified data or software that Applicant and his team could use for analysis. (Tr. 94, 99-103; GE 6 at 7) Technicians were concerned that a file marked unclassified might actually contain classified data. (Tr. 87) The only way classified information could be placed on unclassified computers was through an error in the trusted-download process, or a deliberate improper transfer of classified information. (Tr. 78) Applicant was not authorized to make a trusted download, and he denied knowingly transferring classified information to an unclassified computer. (Tr. 78) There are eight or nine people that could have been responsible for entering data that was too close to the thresholds to be unclassified. (Tr. 214)

Applicant's team's project utilized a classified version and an unclassified version of a computer program. The classified version used "a set of parameters, thresholds, which [were] put together along with the executable part of the program" to generate a "classified result." (Tr. 100, 107) The classified numbers changed as the project advanced. (Tr. 122-123) M was a key person in deciding whether data should be classified or not. (Tr. 128) The unclassified version of the program used numbers that were not representative of the real system to simulate interactions, which allowed use of laptops and communications in an unclassified environment and improved productivity. (Tr. 100-101, 107) The non-representative numbers were used "to test the mechanics of the program" and debug problems in an unclassified environment. (Tr. 108) The classified numbers were not supposed to be used on unclassified computers. (Tr. 112) M assumed the computer he was issued was from Company L and not from DOD. (Tr. 113) The unclassified versions could be used at home. (Tr. 100-102) Employees were allowed to use company-issued computers for some personal use; however, extensive personal use was discouraged. (Tr. 124) At Company L, if a spillage was discovered, Company L's facility security officer (FSO) was supposed to be notified. (Tr. 115) The FSO was responsible for ensuring the file was deleted from computers. (Tr. 116) After deletion of the file, security used a cleaning program to scramble the computer memory.

[1]Unless stated otherwise, the source for the information in this section is a December 16, 2010, letter from an FBI special agent written to the Defense Industrial Security Clearance Office (DISCO) about the investigation of Applicant for unauthorized removal and retention of classified documents or material in possible violation of 18 U.S.C. § 1924. (GE 3)

(Tr. 116) Applicant had access to classified versions of the program and classified program data. (Tr. 118)

Employees of Companies D and L sought to maintain separation between the classified and unclassified versions. (Tr. 101, 106-108) In 2008, the security people interviewed employees and borrowed computers with the programs on their computers to check for a data spill. (Tr. 102) Security found files containing classified information on the computers of four to seven employees of Company L, including on M's computer. (Tr. 102-103, 118-121) Security performed cleansing operations on the computers to eliminate the files with classified information. (Tr. 102-103, 118-121) Because of the spillage, the whole unclassified-simulation program was terminated, and all future simulation work was done on the classified side. (Tr. 119, 124) Team members worked on different areas of the program. (Tr. 104-105) Their work would be subsequently merged, which could cause classified data to be unknowingly transferred from one computer to another, and no one would know the origin of the classified information. (Tr. 104-105)

In December 2007, Applicant received a trusted download onto a flash drive from the Navy for evaluation of Applicant and his team. (Tr. 221; GE 5; GE 6) The information was supposed to unclassified. Classified files from downloads were labeled with a C, and unclassified files from trusted downloads were labeled with a T for test. (Tr. 192) In December 2007, B, a GS-13, who was the senior Navy employee on the team, was at Applicant's residence, when they were doing some computer work. (Tr. 92, 192) Applicant inserted a flash drive into B's laptop computer and was surprised to see a file starting with a C, which meant the file could be classified. (Tr. 193, 217-218; GE 5 at 2) Applicant had previously transferred the data from the flash drive to his DOD-issued laptop computer without noticing the C-file. (Tr. 217) Applicant and B reviewed the content of the C-file and determined it was too "inchoate" and lacked a specification to be classified. (Tr. 193) Nothing inside the C-file was marked classified, and the content of the C-file never made it into a specification. (Tr. 193-194)

In December 2007, the information from the flash drive would have been classified; however, by 2015, it was clear that at most it was sensitive information. (Tr. 194, 220; GE 5 at 2) In 2007, the classification level for the data found on Applicant's computer was probably confidential. (GE 6 at 4) B and Applicant agreed that the file should be deleted, and B suggested that Applicant download a cleaning program to be sure it was deleted. (Tr. 193; GE 4 at 2; GE 6 at 2) They deleted the file. (Tr. 162) Applicant obtained a cleaning program, which wipes out inactive files. (Tr. 195-196)[2] It deletes files from the recycle bin. (Tr. 224) Applicant conceded it was bad judgment to delete the file without going to security. (Tr. 195, 235) Applicant has never had any security violations. (Tr. 195) Applicant did not disclose the possible transfer of classified information to an unclassified system until August 19, 2010 when he met with an

[2]Applicant is not the only team member with a clearing program on his DOD-issued computer. C has a cleaning or deletion program on his computer. (Tr. 80) C understood that if classified information were found on an unclassified computer the safest reaction is to delete the classified information to ensure its protection from loss or compromise. (Tr. 80-81) The spillage should also be reported to the FSO. (Tr. 85-86)

Assistant U.S. Attorney (AUSA) and others for a proffer session. Applicant promised to report any spillage that occurs immediately to his company (FSO). (Tr. 214)

On January 18, 2008, two employees of a rival defense contractor (Company L) told investigators that Applicant may be responsible for the unauthorized removal and retention of classified materials. (GE 4)

On January 28, 2008, Company D's FSO called Applicant and asked him to provide his two DOD-issued laptop computers to Company L. (Tr. 196, 229) One of the requested laptop computers was at Applicant's home. (Tr. 197-199) The FSO did not explain why the computers were requested. (Tr. 199) Applicant said he would bring the computers the next day, and the FSO did not insist or demand that Applicant provide the computer sooner. (GE 6 at 6) Applicant did not believe there had been classified information on the laptop computers. (Tr. 200) Applicant said he deleted some family pictures and other personal information that he did not want to release. (Tr. 139-140, 162-163, 169-170, 202, 227-229) On January 29, 2008, Applicant turned in the two laptop computers. (GE 6 at 2)

In early February 2008, Applicant went to another state where there was a computer with the same program. Two subject matter experts (SMEs), who were associated with Applicant's team, reviewed the "unclassified data" on the hard drive and determined that there was probably classified data on the computer. (Tr. 76-77, 205, 213; GE 6 at 2-3) Most of the information was unclassified; however, the classified information was one table of numbers or parameters, and none of the SMEs were aware of how the classified table had migrated from the classified system to the unclassified system. (Tr. 77, 88, 90, 213, 232-233) In February 2008, Applicant contacted Company D's FSO and advised her of the possibility of confidential data on team computers. The computers were collected to detect any spillage. (Tr. 205-206; GE 6 at 4) One of the SMEs also contacted his FSO about the possible spillage. (Tr. 206)

Applicant consulted a Navy captain, who advised Applicant to seek the assistance of counsel, and in February 2008, he hired a counsel with significant national security experience. (Tr. 203; GE 5 at 2; GE 6 at 4; AE M) On March 4, 2008, Applicant's counsel disclosed to the FBI that Applicant deleted the Company D proprietary files because Company L had requested the computers. (AE B at 2-3)

After receipt of the first two computers, the Naval Criminal Investigative Service (NCIS) and FBI wanted to check a laptop computer and a desk top computer in Applicant's possession for spillage. NCIS requested the two computers in February 2008. (Tr. 141; AE B) Applicant had saved tax returns and other personal information on the desktop computer. The desk top computer was obsolete and lacked sufficient computer power to run simulations, and Applicant believed it had no risk of having classified data on it. (Tr. 210) Applicant's attorney wanted to find out whether the two computers were owned by Applicant, Company D, or DOD before providing them to the FBI or NCIS. (Tr. 141) With the assistance of Company D, Applicant's attorney determined the two computers were probably owned by DOD. On March 4, 2008, Applicant's attorney wrote the FBI volunteering to have Applicant provide the two

computers to the FBI. (Tr. 143-147, 164-165, 226; AE B; AE H) The FBI did not allege that there were deletions from the two computers Applicant provided in March 2008; however, Applicant said the Company D proprietary information that he did not want to release to Company L was on the second set of computers provided to NCIS and the FBI. (Tr. 228-230) Applicant deleted the Company D proprietary information. (Tr. 228-232) Applicant's attorney disclosed to the FBI that she had retained a copy of the hard drive of the desktop computer in her office safe. (Tr. 144; AE B) The FBI never asked for the copy of the hard drive. (Tr. 144-145) There is no evidence that the FBI found any classified information on the two computers provided on March 4, 2008. (Tr. 172)

Investigators checked some of the computers used in the project; however, they did not check all of the other computers used on the project that logically might also have spillage. (Tr. 79, 81, 88-89) C assumed that Company L was out to get Applicant because of how he was targeted by the investigation. (Tr. 82-83) The FBI did not interview C. (Tr. 80)

On August 19, 2010, Applicant and his counsel met with an AUSA and others for a proffer session. (Tr. 149) Applicant advised the FBI that Applicant had compact discs that he received from Company L with trusted downloads for testing simulations. (Tr. 156-159, 210, 212) The discs were marked unclassified. (Tr. 210) Applicant also disclosed he had the flash drive that contained the C-file that he downloaded on his computer in December 2007. (Tr. 222) He had previously deleted the C-file off of the flash drive. (Tr. 224) On August 23, 2010, Applicant provided the requested compact discs and flash drive to the NCIS. (Tr. 159, 170, 222; AE H)

At the August 19, 2010 proffer, AUSA, an FBI special agent, and two NCIS special agents asked Applicant numerous questions about the computers, project, and classified data. (Tr. 150; AE C) The forensic examination determined that classified materials had been stored on one of the laptop computers. FBI SMEs, who were not related to Applicant's team, reviewed the "classified values" and concluded 11 values were not sufficiently scrambled to render them unclassified. (Tr. 213; GE 3; GE 5 at 3; AE P) The classification level was deemed to be confidential. (AE L; AE P) Applicant believed the FBI SMEs erred in the manner that some of the numbers were "reverse engineered" and classified as confidential or secret. (GE 6 at 5) The FBI had been relying on erroneous information from SMEs, and the FBI SMEs had mistakenly confused some of the unclassified testing numbers with classified data. (Tr. 151, 154, 211; GE 3) Applicant agreed with the FBI that one table contained classified numbers. (Tr. 151-154; GE 5 at 2-3) Applicant conceded his unclassified computer should not have been used for classified information because it did not contain the security measures required for storage of classified material. (Tr. 155-156)

The AUSA appeared to accept that Applicant was involved in an inadvertent spill of classified numbers as opposed to a deliberate attempt to compromise classified information. (Tr. 152) On December 16, 2010, an FBI special agent wrote the Defense Industrial Security Clearance Office (DISCO) about the investigation of Applicant for unauthorized removal and retention of classified documents or material in possible violation of 18 U.S.C. § 1924. (GE 3) The FBI letter advised that no charges would be

filed against Applicant; however, the allegations were referred to DISCO for appropriate action. The statute of limitations has now run, and prosecution is barred. (Tr. 153)

From January 2008 to August 2010, the FBI and NCIS did not ask Applicant for any evidence. (GE 6 at 7) On March 4, 2008, Applicant's attorney wrote the FBI and offered to cooperate with the FBI investigation. (AE B) Applicant's attorney indicated Applicant was cooperative with the investigation. (Tr. 160)

Character Evidence

A Navy captain has known Applicant since the late 1990s and served with him on more than one tour at sea. (Tr. 26-27) He has reviewed the SOR and two of Applicant's affidavits related to the SOR. (Tr. 28-29; GE 5; GE 6) He described Applicant as an "incredibly gifted" and "incredibly skilled" technician. (Tr. 29, 34) He is "arguably a genius" and exceptionally creative. (Tr. 34) On one occasion aboard a warship at sea, through Applicant's diligent and inspired efforts, he was able to make a "great breakthrough" with the operation of a vital weapons system. (Tr. 32) Applicant is conscientious about the protection of classified information. (Tr. 33) He recommended reinstatement of Applicant's security clearance through the top secret with access to sensitive compartmented information (TS/SCI) level. (Tr. 37-38)

A high-level DOD employee with TS/SCI access, who has oversight authority over about 9,000 of DOD employees and a $300 million budget, traveled thousands of miles at his own expense to support Applicant. (Tr. 41-43, 52-53) He has known Applicant since the early 1990s. (Tr. 43) He has reviewed the SOR and two of Applicant's affidavits related to the SOR. (Tr. 44-45; GE 5; GE 6) Applicant occasionally discovered design flaws with Company L's work, and some Company L employees resented Applicant. (Tr. 48) Applicant's comments may have cost Company L some award fees that might have otherwise been awarded by the Navy contracting officers. (Tr. 48) Applicant is intellectually gifted, talented, professional, and exceptionally diligent and dedicated to mission accomplishment. (Tr. 50-51) He recommended reinstatement of Applicant's security clearance. (Tr. 55)

A program director on a project has known Applicant since 2003. (AE K) Applicant is open, candid, and honest. (AE K) Applicant was committed to the mission and U.S. national security interests. (AE K) He is aware of the SOR allegations. (Tr. 60, 64-66) Company L employees were having difficulty keeping up with Applicant, and Applicant did not "endear himself" to Company L when he stated his opinions about Company L's work. (Tr. 66-67) He has complete confidence in Applicant's ability to protect classified information and recommends reinstatement of his access to classified information. (Tr. 62, 69; AE K)

The Navy has employed K for 30 years; he is a GS-15 with extensive expertise in simulations and security classification issues; and he has known Applicant professionally since the 1990s. (AE L) He performed the NCIS classification review of the information found on Applicant's laptop computers and was briefed on the investigation. (AE L; AE P) He concluded Applicant's violations of security rules were

inadvertent. (AE L) Applicant provided tireless service to the Navy, and he recommended reinstatement of Applicant's security clearance. (AE L)

C has known Applicant since 1998, and worked with him in 2008. (Tr. 73-79; AE I) C has experience in the same technology as Applicant. (Tr. 76) Applicant has outstanding integrity, and he recommended reinstatement of Applicant's access to classified information. (Tr. 83-84)

M is employed at Company L, and he worked on the 2007-2008 project with Applicant. (Tr. 99-100). M recommended reinstatement of Applicant's security clearance. (Tr. 108, 163)

An attorney with experience as a Defense Investigative Service (DIS) agent and substantial experience in national security law represented Applicant beginning in February 2008. (Tr. 131; AE M) Applicant waived his attorney-client privilege, which permitted the attorney to fully discuss Applicant's communications to her and Applicant's willingness to cooperate with the investigation. (Tr. 135-136) She recommended reinstatement of Applicant's security clearance.

Policies

The U.S. Supreme Court has recognized the substantial discretion of the Executive Branch in regulating access to information pertaining to national security emphasizing, "no one has a 'right' to a security clearance." *Department of the Navy v. Egan*, 484 U.S. 518, 528 (1988). As Commander in Chief, the President has the authority to control access to information bearing on national security and to determine whether an individual is sufficiently trustworthy to have access to such information." *Id*. at 527. The President has authorized the Secretary of Defense or his designee to grant applicant's eligibility for access to classified information "only upon a finding that it is clearly consistent with the national interest to do so." Exec. Or. 10865, *Safeguarding Classified Information within Industry* § 2 (Feb. 20, 1960), as amended.

Eligibility for a security clearance is predicated upon the applicant meeting the criteria contained in the revised adjudicative guidelines. These guidelines are not inflexible rules of law. Instead, recognizing the complexities of human behavior, these guidelines are applied in conjunction with an evaluation of the whole person. An administrative judge's overarching adjudicative goal is a fair, impartial, and commonsense decision. An administrative judge must consider all available, reliable information about the person, past and present, favorable and unfavorable.

The Government reposes a high degree of trust and confidence in persons with access to classified information. This relationship transcends normal duty hours and endures throughout off-duty hours. Decisions include, by necessity, consideration of the possible risk the applicant may deliberately or inadvertently fail to safeguard classified information. Such decisions entail a certain degree of legally permissible extrapolation about potential, rather than actual, risk of compromise of classified information. Clearance decisions must be "in terms of the national interest and shall in no sense be

a determination as to the loyalty of the applicant concerned." *See* Exec. Or. 10865 § 7. This decision is not based, in whole or in part, on any express or implied determination about applicant's allegiance, loyalty, or patriotism. Thus, any decision to deny a security clearance is merely an indication the applicant has not met the strict guidelines the President and the Secretary of Defense have established for issuing a clearance.

Initially, the Government must establish, by substantial evidence, conditions in the personal or professional history of the applicant that may disqualify the applicant from being eligible for access to classified information. The Government has the burden of establishing controverted facts alleged in the SOR. *See Egan*, 484 U.S. at 531. "Substantial evidence" is "more than a scintilla but less than a preponderance." *See v. Washington Metro. Area Transit Auth.*, 36 F.3d 375, 380 (4th Cir. 1994). The guidelines presume a nexus or rational connection between proven conduct under any of the criteria listed therein and an applicant's security suitability. *See* ISCR Case No. 95-0611 at 2 (App. Bd. May 2, 1996).

Once the Government establishes a disqualifying condition by substantial evidence, the burden shifts to the applicant to rebut, explain, extenuate, or mitigate the facts. Directive ¶ E3.1.15. An applicant "has the ultimate burden of demonstrating that it is clearly consistent with the national interest to grant or continue his security clearance." ISCR Case No. 01-20700 at 3 (App. Bd. Dec. 19, 2002). The burden of disproving a mitigating condition never shifts to the Government. *See* ISCR Case No. 02-31154 at 5 (App. Bd. Sep. 22, 2005). "[S]ecurity clearance determinations should err, if they must, on the side of denials." *Egan*, 484 U.S. at 531; *see* AG ¶ 2(b).

Analysis

Personal Conduct

AG ¶ 15 expresses the security concern pertaining to personal conduct:

> Conduct involving questionable judgment, lack of candor, dishonesty, or unwillingness to comply with rules and regulations can raise questions about an individual's reliability, trustworthiness and ability to protect classified information. Of special interest is any failure to provide truthful and candid answers during the security clearance process or any other failure to cooperate with the security clearance process.

Two personal conduct disqualifying conditions under AG ¶ 16 are potentially applicable. Those two disqualifying conditions provide:

> (d) credible adverse information that is not explicitly covered under any other guideline and may not be sufficient by itself for an adverse determination, but which, when combined with all available information supports a whole-person assessment of questionable judgment, untrustworthiness, unreliability, lack of candor, unwillingness to comply with rules and regulations, or other characteristics indicating that the

> person may not properly safeguard protected information. This includes but is not limited to consideration of: . . . (3) a pattern of . . . or rule violations; and
>
> (e) personal conduct, or concealment of information about one's conduct, that creates a vulnerability to exploitation, manipulation, or duress, such as (1) engaging in activities which, if known, may affect the person's personal, professional, or community standing. . . .

AG ¶¶ 16(d) and 16(e) apply. Applicant violated rules in December 2007 when he discovered that he had downloaded possible classified information onto B's computer and his own computer, and he failed to report this security breach to his FSO (SOR ¶ 1.a).

Applicant refuted the SOR allegations in SOR ¶¶ 1.b through 1.e. SOR ¶ 1.b. On January 28, 2008, Company D asked Applicant to return two computers; however, Company D did not indicate it was necessary to return the computers that day. One of the computers was at Applicant's home, and he had other errands to complete that day. Applicant provided the computers the next morning. He had a deletion program running on one of the computers. No rules were violated.

SOR ¶ 1.c. The hard drive of one of Applicant's computers was restricted to unclassified information use, and it was found to contain some classified data. Applicant was unaware his computer contained classified information. He is not responsible for "trusted downloads," and he inadvertently downloaded classified information from a trusted download onto his hard drive. In February 2008, he reported this breach to Company D's FSO. He did not knowingly violate any rules.

SOR ¶ 1.d. On March 4, 2008, Applicant's attorney wrote the FBI that Applicant was willing to cooperate with the investigation. On August 19, 2010, during the AUSA proffer, Applicant mentioned he had compact discs and a flash drive from trusted downloads. Applicant did not believe they contained classified information. On August 23, 2010, Applicant provided the compact discs and flash drive. There is no information that they contained classified information.

SOR ¶ 1.e alleges Applicant had two computers that he provided to his attorney, and his attorney retained them as of December 2010. Applicant had four computers that were requested by Company D. Two were requested on January 28, 2008, and he turned two of them into Company D on January 29, 2008. In February 2008, the NCIS and FBI requested two more computers. Applicant's attorney wanted to find out whether the two computers were owned by Applicant, Company D, or DOD before providing them to the FBI or NCIS. On March 4, 2008, Applicant's attorney wrote the FBI volunteering to have Applicant provide the two computers to the FBI. In March 2008, Applicant turned in the two computers to the NCIS around March 4, 2008.

Further analysis concerning applicability of mitigating conditions is required. The Appeal Board concisely explained Applicant's responsibility for proving the applicability of mitigating conditions as follows:

> Once a concern arises regarding an Applicant's security clearance eligibility, there is a strong presumption against the grant or maintenance of a security clearance. *See Dorfmont v. Brown*, 913 F. 2d 1399, 1401 (9th Cir. 1990), *cert. denied*, 499 U.S. 905 (1991). After the Government presents evidence raising security concerns, the burden shifts to the applicant to rebut or mitigate those concerns. *See* Directive ¶ E3.1.15. The standard applicable in security clearance decisions is that articulated in *Egan*, *supra*. "Any doubt concerning personnel being considered for access to classified information will be resolved in favor of the national security." Directive, Enclosure 2 ¶ 2(b).

ISCR Case No. 10-04641 at 4 (App. Bd. Sept. 24, 2013).

Three mitigating conditions under AG ¶ 17 are potentially applicable:

> (c) the offense is so minor, or so much time has passed, or the behavior is so infrequent, or it happened under such unique circumstances that it is unlikely to recur and does not cast doubt on the individual's reliability, trustworthiness, or good judgment;
>
> (d) the individual has acknowledged the behavior and obtained counseling to change the behavior or taken other positive steps to alleviate the stressors, circumstances, or factors that caused untrustworthy, unreliable, or other inappropriate behavior, and such behavior is unlikely to recur; and
>
> (e) the individual has taken positive steps to reduce or eliminate vulnerability to exploitation, manipulation, or duress.

AG ¶ 16(e) is mitigated by AG ¶ 17(e) because Applicant has fully disclosed his rule violations. Law enforcement, security officials, and his witnesses are well aware of his security-related conduct, and he is not vulnerable to exploitation, manipulation, or duress because of his security-related conduct.

AG ¶¶ 17(c) and 17(d) apply. The only evidence of Applicant's December 2007 security breach was Applicant's self-report; however, his self-report was not timely, as it appears it was disclosed at his August 19, 2010 AUSA proffer. However, Applicant's failure to report the December 2007 security breach is not recent; the security breach was inadvertent; "it happened under such unique circumstances that it is unlikely to recur;" and it "does not cast doubt on Applicant's reliability, trustworthiness, or good judgment." He admitted that he showed poor judgment in December 2007 when he discovered that he had downloaded possible classified information onto B's computer and his own computer, and he failed to report this security breach to his FSO (SOR ¶

1.a). Security needed to assess the scope of the breach of security or spillage, and security was unable to check other computers and determine who was responsible for the "trusted download" that caused the security breach.

Applicant understands the importance of informing security of any security breach or possible security breach, and I am confident he will timely disclosed required information. Personal conduct concerns are mitigated. Even if security concerns are not mitigated under Guideline E, they are mitigated under the whole-person concept, *infra*.

Handling Protected Information

AG ¶ 33 articulates the security concern relating to handling protected information as follows, "Deliberate or negligent failure to comply with rules and regulations for protecting classified or other sensitive information raises doubt about an individual's trustworthiness, judgment, reliability, or willingness and ability to safeguard such information, and is a serious security concern."

AG ¶ 34 provides three disqualifying conditions that could raise a security concern and may be disqualifying in this case:

> (b) collecting or storing classified or other protected information at home or in any other unauthorized location;
>
> (c) loading, drafting, editing, modifying, storing, transmitting, or otherwise handling classified reports, data, or other information on any unapproved equipment including but not limited to any typewriter, word processor, or computer hardware, software, drive, system, gameboard, handheld, "palm" or pocket device or other adjunct equipment; and
>
> (g) any failure to comply with rules for the protection of classified or other sensitive information.

AG ¶¶ 34(b), 34(c), and 34(g) apply. These three disqualifying conditions do not include a requirement that Applicant knew he was downloading classified information onto an unclassified system, and they do not require that he be aware that his unclassified computer systems contain classified information.

SOR ¶¶ 1.a and 1.c discussed previously are cross-alleged under SOR ¶¶ 2.a and 2.c. In December 2007, Applicant discovered that he had downloaded possible classified information onto B's computer and his own computer. The two computers were not authorized for storage of classified information.

The hard drive of one of Applicant's DOD-issued laptop computers was restricted to unclassified information use, and a forensic evaluation and SME review found that his laptop computer contained some data classified at the confidential level. Applicant was unaware this computer contained classified information. He is not responsible for

"trusted downloads," and he inadvertently downloaded classified information from a trusted download onto his hard drive.

Three mitigating conditions under AG ¶ 35 are potentially applicable:

> (a) so much time has elapsed since the behavior, or it has happened so infrequently or under such unusual circumstances, that it is unlikely to recur and does not cast doubt on the individual's current reliability, trustworthiness, or good judgment;
>
> (b) the individual responded favorably to counseling or remedial security training and now demonstrates a positive attitude toward the discharge of security responsibilities; and
>
> (c) the security violations were due to improper or inadequate training.

AG ¶¶ 35(a) through 35(c) apply. As indicated in the previous section, AG ¶ 35(a) is established. The particular simulation program involving inadvertent transfers of classified data to unclassified systems was changed to a completely classified system. Such erroneous "trusted downloads" will not recur. Applicant understands how important it is to avoid future transfers of classified information to unclassified computer systems. He has been counseled and understands that when a security violation is discovered, it should be timely reported to his FSO. He has a positive attitude towards conscientiously complying with security requirements.

Applicant's actions since March 2008 show sufficient effort, good judgment, trustworthiness, and reliability to warrant mitigation of handling protected information security concerns. Even if handling protected information concerns are not mitigated under Guideline K, they are mitigated under the whole-person concept, *infra*.

Whole-Person Concept

Under the whole-person concept, the administrative judge must evaluate an Applicant's eligibility for a security clearance by considering the totality of the Applicant's conduct and all the circumstances. The administrative judge should consider the nine adjudicative process factors listed at AG ¶ 2(a):

> (1) the nature, extent, and seriousness of the conduct; (2) the circumstances surrounding the conduct, to include knowledgeable participation; (3) the frequency and recency of the conduct; (4) the individual's age and maturity at the time of the conduct; (5) the extent to which participation is voluntary; (6) the presence or absence of rehabilitation and other permanent behavioral changes; (7) the motivation for the conduct; (8) the potential for pressure, coercion, exploitation, or duress; and (9) the likelihood of continuation or recurrence.

Under AG ¶ 2(c), the ultimate determination of whether to grant eligibility for a security clearance must be an overall commonsense judgment based upon careful consideration of the guidelines and the whole-person concept. I have incorporated my comments under Guidelines E and K in my whole-person analysis. Some of the factors in AG ¶ 2(a) were addressed under Guidelines E and K, but some warrant additional comment.

Applicant is a 56-year-old software engineer employed by Company D from 1980 to 2007. From 2008 to present, he has been employed by another defense contractor. His spouse is a security clearance holder; his father was a career Navy officer; his two older brothers served in the Navy; and his nephew was a Navy Seal, who served three tours in Afghanistan. In 1982, Applicant received a bachelor of science degree in mathematics. During Desert Shield, Applicant was deployed for six months to the Persian Gulf aboard a U.S. Navy vessel.

A Navy captain, who has known Applicant since the late 1990s; a high-level DOD employee, who has oversight authority over about 9,000 of DOD employees and a $300 million budget and who has known Applicant since the 1990s; a program director on a project, who has known Applicant since 2003; two contractors, who worked with Applicant on the project at issue; and Applicant's attorney described Applicant in laudatory terms. Applicant is an "incredibly gifted," exceptionally creative, and "incredibly skilled" technician and engineer. He is diligent, intelligent, professional, open, candid, honest, and conscientious about the protection of classified information. Most of his character witnesses were aware of the SOR allegations, had read Applicant's statements in 2011 and 2013, and recommended reinstatement of Applicant's security clearance.

Applicant's SOR allegations relate to his handling of confidential information in December 2007 and January 2008 and participation in the follow-up investigation in 2009 and 2010. Company L or Navy employees provided "trusted downloads" to Applicant and his team. The trusted downloads were not supposed to contain classified data or software; however, there was some classified data mixed in with the unclassified data. Applicant and other members of his team unknowingly downloaded the classified and unclassified information onto computers allocated to unclassified information. Applicant did not compromise classified information as there is no evidence the unclassified computers were used by anyone not authorized to review the classified information. In December 2007, Applicant discovered possible classified information on his unclassified computer and on B's computer. B and Applicant agreed that they should delete it, and they did so. This error was aggravated when Applicant and B failed to disclose the discovery of the probable classified information on the flash drive and their computers to their FSOs. Applicant did not receive adequate training or supervision from B, a GS-13 Navy employee on this occasion. There was no evidence that Applicant was told prior to December 2007 of the protocol after discovery of possible classified information on an unclassified computer.

After two of Applicant's assigned DOD-issued computers were requested, he deleted Company D proprietary information and personal information before providing

one computer to Company D and one computer to NCIS. These deletions raised the possibility that he was intentionally obstructing the investigation because forensic examination revealed there were deletions, but could not determine the content of the deletions. Applicant provided the only evidence of the content of the deletions. In February 2008, after Applicant made the deletions, he hired an experienced national security attorney who advised him to cooperate with the investigation. After March 2008, Applicant cooperated with the investigation, and his attorney notified the FBI that he would assist the investigation. His errors in judgment were made from December 2007 through February 2008 and are not recent.

Applicant's hearing statement was credible. He understands what he needs to do to maintain his eligibility for access to classified information. He has avoided any hint of violation of his employer's rules or security rules after March 2008. He expressed sincere remorse for his infractions of security rules and errors in judgment in December 2007 and January 2008, and he emphasized his determination to conscientiously comply with all security rules and requirements. I am confident he will continue to conscientiously exercise his security responsibilities in the future.

I have carefully applied the law, as set forth in *Egan,* Exec. Or. 10865, the Directive, and the AGs, to the facts and circumstances in the context of the whole person. Personal conduct and handling protected information concerns are mitigated, and eligibility for access to classified information is granted.

Formal Findings

Formal findings For or Against Applicant on the allegations set forth in the SOR, as required by Section E3.1.25 of Enclosure 3 of the Directive, are:

Paragraph 1, Guideline E:	FOR APPLICANT
Subparagraphs 1.a through 1.e:	For Applicant
Paragraph 2, Guideline K:	FOR APPLICANT
Subparagraphs 2.a and 2.b:	For Applicant

Conclusion

In light of all of the circumstances presented by the record in this case, it is clearly consistent with the national interest to grant or continue Applicant's eligibility for a security clearance. Eligibility for access to classified information is granted.

_____
Mark Harvey
Administrative Judge