DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
----------	)	ISCR Case No. 14-00498
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Robert J. Kilmartin, Esq., Department Counsel
For Applicant: John M. Smith, Esq.

10/16/2015

Decision

HARVEY, Mark, Administrative Judge:

Applicant's statement of reasons (SOR) alleges 14 violations of security rules. He admitted to nine security-related infractions from March 2012 through October 2013. Applicant's conduct did not result in the compromise of classified or sensitive information.[1] Applicant did not receive adequate training or supervision from his facility security officer (FSO), D, who showed poor leadership and was terminated or resigned from her employment in December 2013. Applicant took over as acting FSO; he obtained extensive security training; and he significantly improved his Department of Defense (DOD) employer-contractor's (C) security. Handling protected information security concerns are mitigated. Eligibility for access to classified information is granted.

Statement of the Case

On April 15, 2010, Applicant submitted an Electronic Questionnaires for Investigations Processing (e-QIP) version of a security clearance application (SF 86). (GE 1) On May 6, 2014, the 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

[1] Department Counsel conceded and Applicant agreed that no spillage or compromise of classified information resulted from the infractions of security rules, and Applicant went to great lengths to education and train himself on security rules and requirements. (Tr. 12-13, 143)

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 alleged security concerns under Guideline K (handling protected information). (HE 2) The SOR detailed reasons why the DOD CAF was unable to find that it is clearly consistent with the national interest to grant or continue Applicant's access to classified information and recommended referral to an administrative judge to determine whether Applicant's clearance should be granted, continued, denied, or revoked. (HE 2)

On July 10, 2014, Applicant responded to the SOR allegations and requested a hearing. (HE 3) On April 29, 2015, Department Counsel was prepared to proceed. On May 7, 2015, the case was assigned to me. On September 3, 2015, the Defense Office of Hearings and Appeals (DOHA) issued a hearing notice setting the hearing for September 24, 2015. Department Counsel offered five exhibits into evidence, and Applicant offered 11 exhibits into evidence. (Tr. 17-20, 47-50; Government Exhibit (GE) 1-5; Applicant Exhibit (AE) 1-11) There were objections to Applicant's exhibits that went to the weight of the evidence, and all exhibits were admitted into evidence. (Tr. 18-20, 47-50) On October 2, 2015, DOHA received the transcript of the hearing. The record closed on October 2, 2015.

Findings of Fact[2]

In Applicant's SOR response, he made detailed admissions about nine of the fourteen incidents alleged in SOR ¶¶ 1.a through 1.n. (Tr. 140) Several of the SOR allegations were duplications of other SOR allegations. He also provided clarifying, extenuating, and mitigating information as part of his SOR response. Applicant's admissions are accepted as findings of fact.

Applicant is a 33-year-old private security specialist and former acting FSO. (Tr. 5-6; GE 1) When he was a senior in college, he received the Reserve Officer Training Corps (ROTC) award for the Marine Corps cadet with the best grades and leadership ratings. (Tr. 52) He graduated from college in 2005. (Tr. 51) He served on active duty as an intelligence officer in the Marine Corps from 2005 to 2010, and he received an honorable discharge. (Tr. 10, 53, 115) In 2008 and 2009, he served in the Marine Corps in Iraq for a total of two tours, and part of his duties involved working with classified documents. (Tr. 51-55) In January 2010, he left active duty; however, he elected to remain in the Marine Corps Reserve. (Tr. 57) He has served in the Reserve as an intelligence officer, and he has been selected for promotion to major. (Tr. 57) His promotion to major is on hold until his security clearance issues are resolved. (Tr. 58) There is no evidence of illegal drug use, criminal offenses, or alcohol abuse. Applicant is married, and his daughter is one year old. (Tr. 112)

[2]Some details have not been included in order to protect Applicant's right to privacy. Specific information is available in the cited exhibits.

In March 2010, C hired Applicant as a security specialist with a focus in operational security. (Tr. 58) From March 2010 to May 2011, his supervisor and rater at C was S. (Tr. 59) He worked on threat assessments involving DOD contractor employees serving overseas and protecting classified documents in overseas facilities. (Tr. 60-62) C has several facilities in the United States and in foreign countries. C's facility where Applicant works is massive. (Tr. 63) It is about a mile long and in some parts about one-quarter mile deep. (Tr. 62-63) It has a fence, guards, video cameras, card-reader systems, and other physical security measures to establish security-in-depth. (Tr. 63)

Applicant has been authorized to be absent from his employment at C on multiple occasions. He was TDY to Korea and otherwise in 2012 and 2013, as well as to a Marine Corps course from March through May 2013. (Tr. 64, 136) He missed some security updates or changes in policy that D issued while he was away from work at C. (Tr. 136-137) On April 5, 2013, D provided Applicant's calendar year (CY) 2012 CY evaluation to Applicant. (AE 8 at 8) The rating cited three security or DOD Manual 5220.22-M, National Industrial Security Program (NISPOM) (Feb. 28, 2006) violations and said Applicant's "understanding of the NISPOM was limited and required extensive education . . . for the last 3 months, your understanding of the NISPOM grew. Continued growth is needed." (AE 8, 2012 CY evaluation at 2, 3) The 2012 CY evaluation also indicated that the 2012 Defense Security Service (DSS) assessment determined that security records were not accurate and "DSS advised that [C] was ineligible for an enhancement credit." (AE 8, 2012 CY evaluation at 2) Applicant acknowledged that his 2012 CY evaluation made him realize it was important for him to improve his knowledge of the NISPOM. (Tr. 65)

Applicant's 2013 CY evaluation showed an overall rating of "Strong Contributor" with performance and growth ratings of "Consistently Meets Expectations." (AE 8, 2013 CY evaluation at 1) His supervisor said, "Additionally, he needs to continue to apply the lessons learned from various security incidents to preclude recurrence. This is especially true in the area of routine security procedures to include end-of-day checks and transmittal of classified materials." (AE 8, 2013 CY evaluation at 5)

In May 2013, Applicant returned from TDY, and he began working diligently to complete security-related courses in addition to working to correct the deficiencies DSS found in their inspection. (Tr. 66) Applicant provided certificates showing he completed 19 security courses from June through July 2013. (AE 7) He completed two additional security courses in January 2015. (AE 7)

In November 2013, D was removed from employment as FSO at C. (Tr. 102) Even though Applicant was not the Assistant FSO, he was appointed as the acting FSO. (Tr. 102) For CY 2014, he received an "Excellent" overall evaluation with "Exceeds Expectation" or "Consistently Meets Expectations" in all categories. (AE 8 at 1-9) C recently promoted Applicant from the Assistant FSO job, and he has resumed his responsibility for threat assessments and training for his employer's overseas offices and personnel. (Tr. 67, 110-112)

Handling Protected Information

Loss of Classified Information

The most serious SOR allegation is Applicant's alleged failure to timely report an engineer-custodian's (EC) loss of three classified documents in June 2012. Under NISPOM paragraph 1-300, when "classified information has been lost or compromised" Contractor employees are required to report the loss to his FSO, and an FSO or the contractor is required to report the loss to the cognizant "Federal authorities." Under NISPOM, paragraph 1-302a, "Contractors shall report adverse information coming to their attention concerning any of their cleared employees." Under NISPOM paragraph 1-303, "Classified material that cannot be located within a reasonable period of time shall be presumed to be lost until an investigation determines otherwise" and must be reported to the cognizant security agency (CSA) in this situation, DSS.

Applicant contended that he and another C security specialist (SE2) timely reported the loss of three classified documents to FSO D, and D denied that he did so. Applicant believed that SOR ¶¶ 1.a, 1.k, and 1.n related to the same alleged security infraction. (Tr. 117-118; SOR response) SOR ¶ 1.n alleges on June 11, 2012, Applicant did not adequately secure classified information, and he did not report missing classified documents in a timely manner. SOR ¶¶ 1.a and 1.k allege that on July 13, 201[2], Applicant was tasked to audit all GSA containers at EC's office, and that Applicant failed to timely report missing classified information to the FSO. (Tr. 117) Applicant and SE2 were directed to inventory eight or nine safes holding classified material in EC's office. (Tr. 76) Some of the classified documents dated to the 1970s. (Tr. 76) EC had occupied the area for decades, was "a pack rat," and his area was "a mess." (Tr. 77) As a result of the audit, numerous unneeded classified documents were shredded. (Tr. 78)

Applicant and SE2 could not locate six documents that should have been in the safes. (Tr. 76) Immediately after the audit, Applicant and SE2 reported to D that the audit had failed to locate three documents; however, D denied that she received any such report from Applicant or SE2. (Tr. 76, 120-121,126) Applicant told an Office of Personnel Management (OPM) investigator that he waited more than 24 hours, but less than 48 hours to report the missing documents to D. (Tr. 126) He also told the OPM investigator that the requirement was to report lost classified documents within 24 hours. (Tr. 125)[3] D told them to work with the custodian of the documents and try to find them. (Tr. 79) EC located three of the six documents; however, they were never able to locate three classified documents. (Tr. 79-80) They presumed the three missing documents were destroyed at some time in the past. (Tr. 79) Another audit was conducted of EC's office in July 2012, and the auditors were unable to locate three classified documents. (AE 11 at 14-19)

[3]Applicant's responses in the OPM interview may have been inaccurate in some details because he did not have an opportunity to review the security documents relating to the incidents. (Tr. 141-142) The documents he subsequently reviewed refreshed his memory of the various security infractions. (Tr. 142) The OPM investigator did not obtain a written statement from Applicant, and instead, the OPM investigator generated a summary of what he believed Applicant told him.

Another security employee of the DOD contractor, SE1, and D, each generated a separate July 13, 2012 report about the loss of the three classified documents by EC. (SE 1's report is AE 11 at 14-19; D's report is AE 11 at 20-23) SE1's report said that at the time of the second audit, on July 9, 2012, six classified documents were missing, and three were subsequently found by EC. (AE 11 at 15 note 3) D said she reported the loss. (AE 11 at 23) However, apparently she did not report the loss to DSS because the DSS agent said at the hearing that she received these two incident reports in June 2013 from D along with the other four reports citing Applicant for security infractions. (Tr. 24-25) SE1's July 13, 2012 incident report indicated on June 12, 2012, Applicant asked EC to look for nine specified missing classified documents. (AE 11 at 15 note 4) SE1 said that she "was unable to find any evidence that [Applicant and SE2] timely advised FSO D of the missing classified [documents], conducted any follow-up with [EC] and/or filed any timely reports with the Defense Security Service." (AE 11 at 15 note 4)

Applicant conceded he should have documented his report of the missing documents, and he should have insisted that D report the loss to DSS. (Tr. 118-119; SOR response) D directed the audit in June 2012, and it is unlikely that she did not ask Applicant and SE1 to report the results of the audit in June 2012. In light of D's failure as FSO to timely inform DSS of the losses of the three Secret-level documents for one year (June or July 2012 to June 2013), and D's termination or resignation from employment with the DOD contractor, I resolve the credibility conflict between D and Applicant against D. D's claim that Applicant and SE2 did not tell D of the loss of classified documents in June 2012 shortly after the audit by Applicant and SE2 is not credible.

A May 31, 2013 JPAS entry for Applicant indicates for July 13, 2012, "No Compromise—Failure to report missing classified information in a timely manner to FSO (Culpability of loss determined to lie with a different employee)." (GE 5) A follow-up June 7, 2013 JPAS entry indicates for "11 June 2012," Applicant "did not adequately secure classified information nor did he report missing classified documents in a timely manner." (GE 5 at 1) D was the author of the JPAS entries.

Security Infractions Unrelated to Loss of Classified Information

SOR ¶ 1.b alleges on October 13, 2013, Applicant improperly mailed classified information to a subcontractor without confirming the address was correct. A security employee of the DOD contractor, SE3, was supposed to generate the documentation to mail a classified package, and Applicant was assisting SE3 with the mailing. (Tr. 95, 100) The package was double wrapped; SE3 put the wrong address on it; and Applicant put the same wrong address on the inside layer of the package. (Tr. 96-97; GE 4 at 2) The inner package had the correct makings for classified materials. (GE 4 at 2) The package went to the correct entity, S (a sub-office of C); however, the address at S for a classified package was different than for an unclassified package. (Tr. 96) There is a cleared person in S's unclassified mailroom to bring packages to the S's classified mailroom when situations like this occur. (Tr. 96-97) In this instance, the cleared person in S's mailroom gave the package to S's FSO, who contacted D. (Tr. 97) The incident report is dated October 21, 2013. (GE 4 at 2)

SOR ¶ 1.c alleges on November 15, 2013, Applicant transmitted a classified CD to S before ensuring it had an approved information system specific to the CD. The incident report is dated November 15, 2013; however, the CD was received at S on October 9, 2013. (GE 4 at 1) Applicant was told to send a classified CD to S, and since he personally knew the addressee from other shipments, he mailed the CD to S. (Tr. 98) S's security officer looked at the DD Form 254 associated with the project, and noted the DD Form 254 lacked "an approved information system specific to the CD." (GE 4 at 1) Accordingly, S's security office was unable to properly log in and accept the CD. (Tr. 98; GE 4 at 1) It took S's security officer from October 9, 2013, to November 5, 2013 to review his installation's DD Form 254. (GE 4 at 1) On November 14, 2013, after discussing the matter with D, S's security officer mailed the CD back to Applicant's security office. (Tr. 98-99; GE 4 at 1) Applicant believed S's DD Form 254 was subsequently changed, and the CD was re-mailed back to S. (Tr. 99)

SOR ¶¶ 1.d and 1.e allege on May 14, 2013, and May 22, 2013, Applicant failed to fully complete end-of-day checks on GSA security containers that contained classified material at the Secret level. (AE 11 at 1-5) Applicant conceded that after checking to ensure all safes were locked, he failed to initial and date the SF 702s on the top of one of the safes on two dates in May 2013. (Tr. 93-94) The incident report is dated May 17, 2013. (AE 11 at 1-5) D also said in the incident report that she would enter this report in JPAS. (AE 11 at 2-3)

SOR ¶ 1.f alleges on March 7, 2013, Applicant inadvertently provided incorrect security information involving his authorization of cellular phone possession in C's reproduction room. Applicant erroneously believed cell phone possession was unrestricted; however, cellular phone possession was actually prohibited. C had a room with "millions" of documents in it, and C hired a subcontractor to organize the documents. (Tr. 90-91) A document classified at the confidential level was discovered in the room. (Tr. 90) There was a sign inside the room indicating cell phones were supposed to be placed in a box. (Tr. 91) Applicant did not know whether or not the area was restricted for cell phone possession or not. (Tr. 91-92) Applicant had not seen documentation on whether it was a restricted area or not. (Tr. 90-92) In March 2013, D advised Applicant that the area was restricted and cell phone possession was not permitted. (Tr. 93) Applicant conceded he gave incorrect information to contractors about possessing cell phones in the restricted room. (Tr. 134)

SOR ¶ 1.g alleges on February 19, 2013, Applicant failed to engage an S&G lock on a closed area, containing material at the Secret level, thereby leaving the area alarmed but unlocked for nearly 26 hours. Applicant was called and asked to escort fire inspectors inside a room containing classified material at the Secret level to check a gas line. (Tr. 87; GE 3 at 1-4) After the fire inspectors were done, they exited the room. (Tr. 88) Applicant spun the dial, and heard the lock click once. (Tr. 88; GE 3 at 2) He pulled the handle on the door, and the door was locked. (Tr. 88) He checked the alarm by calling the guards, and they alarmed the door. (Tr. 88-89; GE 3 at 2) Applicant failed to sufficiently spin the dial for two clicks to occur, and the lock was not fully engaged. (Tr. 89) Applicant learned there was a written report on his failure to fully engage the S&G

lock when they were cleaning out D's office and discovered a file with a report on this incident in it. (Tr. 89-90) The report was dated February 22, 2013. (GE 3 at 1-4)

SOR ¶ 1.h alleges on February 12, 2013, Applicant failed to alarm a secure COMSEC area, containing material at the Secret level, thereby leaving the area locked but unalarmed for over four hours. One of the rooms that the scheduled end-of-day security person is supposed to check has a unique lock and alarm system. (Tr. 84-87) At the end of the day, Applicant checked the door and noted the SF 702 was already completed by a user of the room, as they are supposed to do when the last person leaves for the day. (Tr. 84-87) He spun the dial on the lock and pulled the door handle, to ensure the door was properly locked. (Tr. 85-86) The alarm sign was flipped, indicating the alarm was engaged. (Tr. 85-86) Applicant would have had to open the door, set the alarm, exit the room, and lock the door. (Tr. 86) He elected to rely on the alarm sign being flipped, and the user's initials and date on the SF 702 instead of personally entering the room and checking the alarm system. The incident report is dated February 18, 2013. (GE 3 at 9-10; *See* SOR ¶¶ 1.i and 1.j)

SOR ¶ 1.i alleges on September 17, 2012, Applicant failed to complete end-of-day checks on two GSA security containers. Applicant was responsible for checking to ensure approximately 17 GSA safes were secured at the end of the day. (Tr. 82) The safes are in a row, and Applicant is sure he spun each of the dials to ensure they were locked; however, he failed to initial and date the SF 702s on two safes. (Tr. 83, 134; AE 11 at 11) The logs are dated from June through September 2012, and the logs for one of the safes do not have initials and dates for several end-of-day checks which are in a separate column on the SF 702. (AE 11 at 7-10, 13) There are initials and dates in the user column. (AE 11 at 7-10, 13)

SOR ¶ 1.j alleges on August 7, 2012, Applicant failed to complete end-of-day checks on a closed area for four out of five assigned days. Applicant was scheduled to check 17 safes at the end of the day to ensure they were locked, and he was required to initial and date each SF 702s, which were on top of each safe. (Tr. 79-80) D had a safe in her office. (Tr. 81) D's policy was to check her own safe before leaving for the day, and then she would initial and date her safe's SF 702 before locking her office door and going home. (Tr. 81) See, e.g, SF 702 in AE 11 at 7-10, 11. Applicant checked D's office door and noted that it was locked before he left at the end of the day. (Tr. 81) Applicant did not have a key for her office. (Tr. 81, 134) In August 2012, D reminded Applicant that her policy required the scheduled end-of-day security check to include her office safe. (Tr. 82, 135) From the example SF 702's provided, it appears the end-of-day checks in some C locations may have been inconsistently initialed. (AE 11)

SOR ¶ 1.l alleges on March 12, 2012, Applicant did not properly safeguard information classified at the Secret level. SOR ¶ 1.m alleges on March 16, 2012, Applicant mishandled information classified at the Secret level. Applicant believed SOR ¶¶ 1.l and 1.m relate to the same incident. (Tr. 68, 122)[4] Applicant had just begun

[4] The Office of Personnel Management (OPM) personal subject interview (PSI) indicates there were two discrete security infractions in March 2012. One involved failing to supervise contractor

working for D. (Tr. 68) Applicant and another contractor employee went to the post office; they picked up a double-wrapped package containing classified information; and they brought the package to C's security office, which is locked and alarmed. (Tr. 68, 74) The package was too large to fit in the GSA safe in the security office. (Tr. 68) Applicant placed the double-wrapped package in the storage unit or closet and went to lunch with another employee of C. (Tr. 68-69, 74) DSS has certified the closet as a certified closed space on a DD Form 147, and it is locked and alarmed when the door is closed. (Tr. 69) The closet is located in the center of the security area, which is a closed office space. (Tr. 69) The closet already contained numerous classified items as well as supplies and two GSA-approved safes. (Tr. 69)

D generated a document, dated March 16, 2012, indicating Applicant left packages containing Secret-level information "on top of a safe in an area not approved for open storage;" however, D also reported that the documents were "sitting in the vault." (AE 11 at 24) D said her remedy was to discuss the matter at length with Applicant. (AE 11 at 26) D said the DD Form 147 showed the room was not cleared for open storage; however, Applicant said he believed the room was cleared for open storage, and that DSS had inspected the room and numerous classified items were being stored as though the room was open storage. (Tr. 73-74) About two months later, the DD Form 147 was changed to reflect open storage in the security area. (Tr. 75) The incident report is dated March 16, 2012. (AE 11 at 24-26)

Statement from an Industrial Security Specialist (ISS) from the DSS

A DSS ISS (P) described her oversight responsibility of C's facility security. (Tr. 20-21) P has a master's degree and five DOD security-related certifications, and P has worked in security for eight years. (Tr. 21-22) The FSO at Applicant's company was responsible for training employees and security personnel in security matters. (Tr. 22) In June 2013, D provided materials on Applicant's six security-rule infractions to DSS as part of the annual vulnerability assessment. (Tr. 24-25) P said D was not required to provide the information about Applicant to DSS earlier when the infractions occurred because there was no evidence of a compromise or suspected compromise of classified information. (Tr. 24-25)[5] D never disclosed any security infractions for which she was culpable. (Tr. 44) P explained that a DOD regulation required the holder of classified information: to properly transmit classified CDs; to conduct security checks; and to properly set cipher locks. (Tr. 27) The FSO is responsible for security in their assigned facility. (Tr. 28-31) D's supervisor informed DSS that D was terminated or resigned from her employment at C on December 6, 2013, and Applicant became the FSO. (Tr. 28-31, 138, 143; GE 2 at 12)

DSS did not object to Applicant's appointment as FSO. (Tr. 31) Applicant frequently consulted with DSS and P on security matters. (Tr. 31) DSS polls showed

---

employees that were moving documents. (Tr. 123) The other incident involved leaving classified materials on top of a safe. (Tr. 124)

[5] P did not explain why the losses of three classified documents were not reportable.

that increased communications between FSOs and DSS improved facility security. (Tr. 32) Applicant invited DSS to tour C, and he asked DSS to make suggestions about how to improve security. (Tr. 32) C had both open and closed storage areas. (Tr. 34) In an open storage area, a classified package can be left unattended in an "open-shelf bin storage" area. (Tr. 41) After Applicant took over as FSO, DSS noted that his company attempted to gain 100 percent accountability of all classified materials. (Tr. 35) There were thousands of classified documents, and some of which were decades old. (Tr. 35) There is no requirement to maintain accountability for Secret information—the requirement is to maintain accountability for Top Secret and higher-level information. (Tr. 45)

After a DSS assessment in November 2014 to ensure NISPOM compliance and improve security, Applicant's company received a superior rating from DSS. (Tr. 38; AE 5) DSS wrote that C's "SUPERIOR" rating was based on five accomplishments: (1) Applicant's company sponsored an event involving the FBI and DSS; (2) additional annual security training opportunities for employees were made available; (3) a 100 percent inventory of classified holdings and removal of unused documents was completed; (4) Applicant's facility provided fingerprinting for other cleared companies in the area; and (5) security personnel upgraded their certifications and participated in security-related organizations. (AE 5) A superior rating from DSS is reserved for about ten percent of the best facilities in the area of security. (Tr. 106)[6] Applicant was unaware of whether C previously received a superior rating. (Tr. 106)

Applicant received training at DSS' Center for the Development of Security Education, which provides the best security training in DOD. (Tr. 39-40) P said that Applicant, "had a very good relationship [with P] and he performed the duties as required." (Tr. 42) When Applicant became the FSO, he "maintain[ed] contact with [P], regarding any type of clarification on any of the requirements." (Tr. 42)

Applicant received extensive training on security procedures. (Tr. 102) In November 2013, when he became acting FSO, he took action to correct deficiencies. (Tr. 102) He emphasized training of security personnel and C's employees in security matters. (Tr. 103) He frequently briefed P at DSS about his priorities and plans for improving security. (Tr. 104) P and her replacement at DSS advised him on measures to improve security. (Tr. 105) Applicant and the other security personnel worked diligently to improve security in all areas. (Tr. 107-110) They emphasized attention to detail. (Tr. 110) In August 2014, Applicant's employer hired a new FSO. (Tr. 105)

Applicant admitted that he made mistakes, and he expressed sincere remorse for his errors. (Tr. 114, 145) He emphasized his determination to improve, avoid future errors, and establish his trustworthiness. (Tr. 114) He understands the relationship of security and protection of national security, and he takes security matters very seriously. (Tr. 144)

[6] In FY 2012, 8.3% of facilities received a superior rating from the Defense Security Service. (AE 2 at 2)

Character Evidence

Applicant provided 12 character statements from friends, coworkers, supervisors, corporate counsel, an active duty Marine Corps major, his pastor, and an associate pastor.[7] The statements describe his Marine Corps service in peace and war, his work for C, and his personal life. They laud his dedicated service to the Marine Corps and his support for his family, church, and employer. The statements emphasize his diligence, professionalism, efforts at security improvement, conscientious compliance with rules, dependability, loyalty, honesty, trustworthiness, and contributions to mission accomplishment.

Applicant provided his Marine Corps fitness reports. (AE 9) The trend shows improving duty performance. (AE 9) His 2013 fitness report describes an officer, who is "one of the few exceptionally qualified Marines" on the comparative assessment. (AE 9) He is on the promotion list for major.

Applicant has the following military awards: two Iraq Campaign Medals; two Sea Service Deployment Ribbons; three Certificates of Appreciation; one Global War on Terrorism Service Medal; two Navy Unit Commendations; one Navy and Marine Corps Achievement Medal; one Navy and Marine Corps Commendation Medal; and one National Defense Service Medal. (AE 10) He completed several Marine Corps training courses, and he received several certificates of achievement. (AE 10)

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.

Eligibility for a security clearance is predicated upon the applicant meeting the criteria contained in the 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

[7] The source for the information in this paragraph is AE 6.

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. Thus, nothing in this Decision should be construed to suggest that I have based this decision, in whole or in part, on any express or implied determination about applicant's allegiance, loyalty, or patriotism. It 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 [or her] 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

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 two disqualifying conditions that could raise a security concern and may be disqualifying in this case: "(g) any failure to comply with rules for the protection of classified or other sensitive information;" and "(h) negligence or lax security habits that persist despite counseling by management."

Applicant admitted to nine security-related infractions from March 2012 through October 2013. D occasionally mentioned errors Applicant made to him and urged corrective action. Although he did not make the same error after being counseled, he made additional different security errors.

On April 5, 2013, D provided Applicant's evaluation for CY 2012 to Applicant. The 2012 CY evaluation cited three security or NISPOM violations and said Applicant's "understanding of the NISPOM was limited and required extensive education . . . for the last 3 months, your understanding of the NISPOM grew. Continued growth is needed." The 2012 CY evaluation also indicated that the 2012 DSS assessment determined that security records were not accurate. His rating constitutes the only written counseling he received. The rating does not mention "lax security habits" or negligence. The rating emphasized that Applicant needed training on the NISPOM.

After he was counseled in his 2012 CY evaluation on April 5, 2013, he was involved in two more security incidents. In October 2013, he was involved in two mistakes involving the mailing of classified material. The October 2013 mailing of classified material that went to an incorrect mailroom was not his fault as another employee addressed the package and completed the transaction documentation. In October 2013, he mailed a CD without adequate coordination with the security office receiving the CD. Although no specific provision of the NISPOM or any other security rule is cited, I conclude that Applicant should have known that he or someone in the security office should call ahead and let the receiving security office know what type of classified material is about to arrive at their office. He should not have relied on the requestor to properly coordinate the transfer. AG ¶¶ 34(g) and 34(h) apply.

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.

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).

AG ¶¶ 35(a) through 35(c) apply. Applicant realized it was important for him to improve his knowledge of the NISPOM. As soon as he returned from his TDY in May 2013, he worked diligently to complete numerous security related courses in addition to working assiduously to correct the deficiencies DSS found in their inspection. Applicant was not responsible for the loss or compromise of any classified or sensitive information. Much of the responsibility for the infractions was due to Applicant not receiving adequate training or supervision from FSO D, who showed poor leadership and was terminated or resigned from her employment at C in December 2013. Applicant took over as security manager, and he significantly improved C's security and his own security performance.

Applicant's actions since returning from TDY in May 2013 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 AG ¶¶ 35(a) through 35(c), 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 Guideline K in my whole-person analysis. Some of the factors in AG ¶ 2(a) were addressed under Guideline K, but some warrant additional comment.

Applicant is a 33-year-old private security specialist and former acting FSO, who is currently focused on operational security at C. In November 2013, Applicant was appointed as the acting FSO. The DOD contractor recently promoted Applicant, and he is again responsible for threat assessment and training for his employer's overseas offices and personnel. When he was a senior in college, he received the ROTC award for the Marine Corps cadet with the best grades and leadership ratings. He graduated from college in 2005, and he served on active duty in the Marine Corps from 2005 to 2010, as an intelligence officer. He served two tours in Iraq with the Marine Corps. In January 2010, he left active duty; however, he elected to remain in the Marine Corps Reserve. He has served in the Reserve as an intelligence officer, and he has been selected for promotion to major.

Applicant's 12 character statements from friends, professional colleagues, and his pastor emphasize his diligence, professionalism, efforts at security improvement, conscientious compliance with rules, dependability, loyalty, honesty, trustworthiness, and contributions to mission accomplishment. There is no evidence of illegal drug use, criminal offenses, or alcohol abuse.

Applicant's SOR alleges 14 violations of security rules. He admitted to nine security-related infractions from March 2012 through October 2013. Applicant's conduct did not result in the compromise of classified or sensitive information. He did not receive adequate training or supervision from his FSO, D, who showed poor leadership and was terminated or resigned from employment with C in December 2013. Applicant took over as FSO; he obtained extensive security training; and he significantly improved C's security. C achieved a superior security rating from DSS, which is attributed in part to Applicant's leadership and diligent efforts to improve security.

Applicant understands what he needs to do to maintain his eligibility for access to classified information. He has avoided any hint of violation of security rules since October 2013. He expressed sincere remorse for his infractions of security rules 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. 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 K:	FOR APPLICANT
Subparagraphs 1.a through 1.n:	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