DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 17-00796
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Andre M. Gregorian, Esq., Department Counsel
For Applicant: Heather Tenney, Esq.

04/12/2018

_____

Decision

_____

MATCHINSKI, Elizabeth M., Administrative Judge:

Applicant was found culpable by his employer of five separate security violations between November 2009 and November 2015, including of drafting an email containing classified information on an unclassified computer system. He has made some changes to minimize the risk of recurrence, but some doubts persist about his ability and willingness to comply with security regulations. Clearance is denied.

Statement of the Case

On May 23, 2017, the Department of Defense Consolidated Adjudications Facility (DOD CAF) issued a Statement of Reasons (SOR) to Applicant, detailing the security concerns under Guideline K, handling protected information, and explaining why it was unable to find it clearly consistent with the national interest to grant or continue his access to classified information. The DOD CAF took the action under Executive Order (EO) 10865, *Safeguarding Classified Information within Industry* (February 20, 1960), as amended; DOD Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (January 2, 1992), as amended (Directive); and the *Adjudicative Guidelines for Determining Eligibility for Access to Classified Information* (AG) effective within the DOD on September 1, 2006.

On June 29, 2017, Applicant answered the SOR and requested a hearing before an administrative judge from the Defense Office of Hearings and Appeals (DOHA). On September 22, 2017, the case was assigned to me to conduct a hearing to determine whether it is clearly consistent with the national interest to grant or continue a security clearance for Applicant. On October 30, 2017, I scheduled a hearing for December 4, 2017. In prehearing guidance, Applicant was informed that the Director of National Intelligence (DNI) had issued Security Executive Agent Directive 4 establishing the National Security Adjudicative Guidelines (AG) effective June 8, 2017, for all adjudications for national security eligibility or eligibility to hold a sensitive position.[1]

I convened the hearing as scheduled. Three Government exhibits (GEs 1-3) and six Applicant exhibits (AEs A-F) were admitted into evidence without objection. Two hearing exhibits (HE) were marked but not entered into evidence: a July 31, 2017 letter forwarding discovery of GEs 1-3 to Applicant (HE 1) and a list of the Government's exhibits (HE 2). Testimony was taken from Applicant and four witnesses, as reflected in a transcript (Tr.) received on December 12, 2017.

Summary of SOR Allegations

The SOR alleges under Guideline K that Applicant committed five security violations in that he sent an email containing classified information on an unclassified server in November 2009 (SOR ¶ 1.a); failed to properly secure a security container containing classified information in August 2012 (SOR ¶ 1.b); placed classified information relating to a foreign government on an unclassified server in October 2012 (SOR ¶ 1.c); left classified documents unattended in an area not approved for open storage in March 2015 (SOR ¶ 1.d); and sent an email containing classified information via an unclassified server in November 2015 (SOR ¶ 1.e).

In a detailed response, Applicant described his violations as "incidental when considering his more than 30 years of reasonable security behavior and his overall character of integrity, trustworthiness, and reliability." He admitted the violations alleged in SOR ¶¶ 1.a, 1.b (he shut the container but failed to spin the lock), 1.c (he failed to discover the foreign government information in headers and footers before downloading an Excel spreadsheet), and 1.d (he left classified documents unattended in a closed work area). Applicant denied SOR ¶ 1.e (he typed "potentially" classified information in an email, but he never sent the email).

Findings of Fact

After considering the pleadings, exhibits, and transcript, I make the following findings of fact.

[1] Application of the AGs that were in effect as of the issuance of the SOR would not change my decision in this case.

Applicant is a 60-year-old senior systems engineer with his bachelor's and master's degrees in electrical engineering. He has worked in his defense-contractor employment since March 1983, staying on through several corporate mergers. Applicant has held a DOD Secret clearance for approximately 35 years. After graduating from college in 1979, he worked for a small defense contractor for almost four years, and he was granted his first clearance in 1981 or 1982. He has had a successful career and holds one patent. His work performance over the past five years has met or exceeded his employer's expectations. (GEs 1-2; Tr. 26-29, Tr. 28-29, 31.)

Applicant and his spouse have been married since September 1985. They have a 29-year-old daughter, who is married and pursuing her own career as a physician. She has a young son and is expecting her second child in March 2018. (GE 1; Tr. 25.) Applicant and his spouse purchased their present residence in March 1987. (GE 1.) Applicant has been active in his church. He served as an elder and chaired on an interim basis his congregation's search for a new pastor in 2003. (AEs C, E.)

As required for his security clearance, Applicant received annual security briefings from his employer. (Tr. 49.) Applicant's employer found him culpable of violating security procedures in early November 2009. Applicant sent an email containing classified Secret technical data on his employer's unclassified computer network. Applicant explained at his hearing that, while communicating with another engineer about one of the classified parameters on their system, he "inadvertently" put on an unclassified system a value associated with a classified parameter. The receiving engineer noted the violation and reported it. Applicant's work computer, which was not approved for classified processing, was confiscated and cleansed. Applicant denies any compromise of classified information or of any damage. He received a security violation for the incident and was required to complete security-refresher training. (GEs 2-3; Tr. 33-34, 51-52.)

Applicant has worked since at least 2012 in a program-specific closed area not authorized for open storage of classified material. Within the closed area are approved safes for the storage of classified material. Applicant had privileges to access one of the classified containers. On August 15, 2012, Applicant neglected to properly secure a safe for classified storage that he had accessed that day. Applicant had closed the container but accidentally failed to spin the cipher-lock. The violation was discovered during end-of-day security checks by another employee, who reported it to their security office. Applicant was the last one to initial a card noting he had closed the container. His employer found him culpable for the security violation. To Applicant's recollection, an inventory accounted for all classified material. In retrospect, Applicant attributed the violation to being in a hurry. Since the incident, he has taken steps to slow down and make sure that he followed all the steps required to secure the container. (GEs 2-3; Tr. 34-36, 52-54.)

Applicant accepted the responsibilities of being a trusted download for classified information from a server that contained Secret/NOFORN/FGI,[2] and he received some

[2] NOFORN is the acronym for information Not Releasable to Foreign Nationals and FGI is the acronym for

training on his responsibilities in that regard. On October 30, 2012, Applicant placed classified FGI on an information system approved for Secret/NOFORN but not for FGI.[3] He spent about an hour reviewing an Excel spreadsheet to sanitize it of FGI. He removed markings that identified the foreign government but failed to note before the Excel spreadsheet was uploaded to a Secret/NOFORN system that headers and footers contained FGI, which revealed the foreign nation involved. The violation was discovered several months later by an engineer, who reported it to company security officials. Applicant was found culpable for the violation, and he lost his trusted download privileges as a result. The server was upgraded to Secret/NOFORN/FGI because of his violation. (GEs 2-3; Tr. 37-38, 56-57.)

To renew his security clearance eligibility, Applicant completed and certified to the accuracy of a Questionnaire for National Security Positions (SF 86) on February 19, 2014. He responded negatively to the following employment inquiry: "For this employment, **in the last seven (7) years** have you received a written warning, been officially reprimanded, suspended, or disciplined for misconduct in the workplace, such as a violation of security policy?" (GE 1.)

Applicant was interviewed by an authorized investigator for the Office of Personnel Management (OPM) on April 21, 2014. After confirming all the information provided on his SF 86, Applicant then volunteered that he had received four security violations within the last seven years that he failed to report on his paperwork because he misunderstood the employment inquiry to pertain to disciplinary actions that led to suspension or loss of pay. He discussed the incidents involving him entering a document containing Secret data onto an unclassified data storage system; his failure to lock a safe in a closed area; and, in 2012, his "inadvertent" transmittal of an Excel document onto a secure no-foreign classified information system. Applicant reported another incident where, in 2011, he entered a document into an unclassified data storage system that contained frequency information which, when taken as a whole, could provide enough information to decipher classified information. He now understands that he should have asked for a review by security of the frequency information on the classified server before placing it on an unclassified system. The incident was not brought to his attention until 2014. (GE 2.)

On March 2, 2015, Applicant accidentally left a set of working papers classified Secret out on his desk, which was located inside a closed work area not approved for open storage. Applicant recalls that the set of classified working papers was in a manila folder and unattended for about an hour. He was not sure at the time whether it was a violation, but he reported the incident to his security office approximately two hours

---

Foreign Government Information under DOD 5220.22-M, *National Industrial Security Program Operating Manual* (NISPOM), dated February 28, 2006. Applicant recalled the incident as occurring in March 2013, but his employer reports that the incident occurred in October 2012.

[3] Applicant recalled the incident as occurring in March 2013, but his employer reports that the incident occurred in October 2012.

later. He was found culpable for the security violation by his employer and reminded of his obligation to attend to classified material. (GEs 2-3; Tr. 38-39, 57-59.)

On November 11, 2015, Applicant was found culpable by his employer for a security violation. He had drafted a classified email on his unclassified computer, which caused contamination of the local area network (LAN) and compromise of classified information. On reviewing the email containing the classified information, Applicant recognized that he had included a classified parameter in the email. The classified nature of the parameter was "pretty plain in the classification guide." He did not send the email.[4] He locked his computer, and reported the incident to security officials. His computer was taken and scrubbed to expunge any classified data. In January 2016, Applicant received a written security violation. He had to discuss his history of security violations with his facility security officer (FSO), his supervisor, and a human resource employee. Concern was expressed to him about his pattern of security violations. He was advised to be more careful in the future. He was also told to review the security classification guide and refer to a subject-matter expert when needed. A review of his work time for the previous five years showed that he had regularly worked more than 40 hours. His employer limited his work week to 40 hours to minimize the stress of trying to meet the obligations of his program. (GEs 2-3; Tr. 39-40, 43-44, 59-62.)

Applicant was interviewed by a different OPM investigator on December 5, 2016. He volunteered that there had been multiple security violations at work that he had not listed on his SF 86 because he misunderstood the question regarding disciplinary actions and he thought it was not necessary to list them because they were not serious enough to document on his SF 86. About the latest violation in November 2015, he explained that he had typed an unclassified email on an unclassified system and "inadvertently" added classified information, but he also indicated that he had been in a hurry and "careless." Classified information was compromised due to the incident. Applicant also disclosed a cell phone violation that occurred more than seven years ago. He had brought his personal cell phone into a secure work area two days in a row. He explained that he had forgotten to remove his cell phone from his bag. He self-reported his conduct to his security office. (GE 2.)

Applicant provided further details and some corrections about the security incidents to DOHA in April 2017. He admitted that he should have listed his security violations on his SF 86. Regarding the specific incidents, he admitted that he knew bringing a cell phone into a closed area was in violation of security requirements and that he should have reported the incident immediately. Concerning his placement of classified information in an email in November 2009, and on an unclassified server in November 2015, he related that he would take a stricter position on transmitting

[4] The SOR alleges that Applicant sent an email containing classified information on an unclassified server (SOR ¶ 1.e). Applicant denies that he sent the email because he recognized and immediately reported his violation. In reporting Applicant's violations to DOHA in April 2017, the FSO indicated that Applicant "drafted an email containing classified Secret information on his Unclassified System." He does not dispute that he drafted an email containing classified information on a system not approved for classified information.

technical information "on the unclassified email unless it is necessary and conduct a better review [of] the data prior to writing it." He acknowledged about the 2011 security incident involving frequency information that he should have asked for a security review before placing the data on an unclassified system. As for his failure to lock the security container in August 2012, he expressed that he would take more care to secure the container. Regarding the incident where he placed FGI material on a non-FGI server, he acknowledged in retrospect that he should have asked for specific instructions on cleansing the file and should have had another classification reviewer examine the file. Concerning his failure to properly secure his classified working papers in March 2015, he admitted that he knew leaving classified information unsecured was a violation and that he should not have waited to report it. To avoid recurrence, he would put out a reminder when classified material is on his desk. Applicant attributed his security violations to being overconfident in his ability to determine classification; to being in a rush and getting careless; to failing to verify that he was not carrying prohibited material when entering a closed area; and to not taking security sufficiently seriously. Applicant promised to take corrective actions to ensure against recurrence, and he outlined specific measures. (GE 2.)

Applicant continues to support a specific program with access at the Secret/NOFORN level. (Tr. 64.) He admits that he had not done a good enough job safeguarding and protecting classified information over the last eight years, but he denied that any of his violations were deliberate. He cared about complying with security requirements. (Tr. 32-33, 47.) Regarding corrective action, he removed himself from access privileges to the classified container in his work area, and from classification review duties in the past year. When generating classified working papers, he obtained appropriate cover sheets and dated them, put a sign near the entry to his cube to remind him that he had classified information out, and when he was finished, he saw to its destruction by the FSO's office. He consulted with subject-matter experts for guidance in determining whether to classify information. Applicant has not committed a security violation since November 2015. He acknowledges that he was not always open and transparent about his security shortcomings in the past, but that it is important to do so to avoid developing a cavalier attitude about security. (Tr. 36-37, 41-42, 44-45, 48-49, 64.)

Applicant enjoys his work and wants to keep his clearance so that he can continue to contribute to the United States defense. (Tr. 45.) His volunteer activities outside of work usually involve his faith and church-related activities. He had a short stint mentoring some at-risk boys for a local high school. (Tr. 29-31.)

Character References

Applicant presented no work references or performance evaluations. His employer has a strict policy about releasable information. He testified he was not allowed to have co-workers testify "because of the assumed liability of any statements that they may make to the company." (AE A; Tr. 29.)

Four friends authored character reference letters for Applicant. Three of the friends also testified. As noted below, they endorse Applicant for security clearance eligibility, although none appears to be aware of the details of the Government's security concerns.

A longtime friend of Applicant's since high school described Applicant as being a person of integrity and honor. Applicant had not discussed the specifics of his work, other than to indicate that it was challenging. Applicant did not share with him the issues that led the Government to question his security clearance eligibility, although he gave his friend the impression that he was being treated fairly and professionally. This friend learned about a couple of the security issues from Applicant's attorney in preparation for his testimony. This friend has never considered Applicant to be careless. (AE B; Tr. 95-98.)

A friend who has served as a pastor, and is a certified Christian conciliator, held a Secret-level security clearance when he served in the U.S. military during the Vietnam War. He came to know Applicant in 2003 as an elder and interim chairman of the pastor search committee that brought him to serve Applicant's church for 2.5 years. Applicant earned his friend's admiration for his "attention to detail, loyal and conscientious work ethic, wise leadership, and absolute personal integrity." (AE C.)

Another friend, who first met Applicant in 1980 when they volunteered as mentors for a youth group for over five years, resumed the friendship when he moved back to the area in 1988 after graduate school. He and Applicant socialize every other week. He trusts Applicant's discretion and judgment. Applicant has demonstrated "exceptional qualities and character traits" for decades. Although the friend indicated that he cannot speak for Applicant's work situation, he was made aware about a week or so before Applicant's hearing that the security concerns involve Applicant not following company security policies involving information in emails, documents left on a desk unattended, and a safe not secured properly. (AE D; Tr. 87-90.)

A friend of 25 years, who served with Applicant for several years on their church's Board of Elders, attests to the various community service projects they participated in together. Applicant was meticulous in performing time-consuming and detail-oriented duties when their church split and decided to merge with another congregation. This friend described Applicant as "careful to a fault." While Applicant may have made some mistakes, this friend believes they were never intentional or through carelessness or neglect. This friend testified to having "only cursory" knowledge of the issues Applicant had at work. Just before Applicant's hearing, he learned that Applicant did not close a safe and that he sent an email that he should not have sent. (AE E: Tr. 81-84.)

An insurance professional for the past 33 years, who also has 20 years of experience as a lay pastor, has known Applicant through their church. In his opinion, Applicant possesses integrity and discretion, and has demonstrated "great discipline and conscientious execution of his responsibilities." He was surprised to learn that

Applicant's clearance was under review and would attribute any lapse in Applicant's attention to regulation, to a heavy workload, and to long hours. He believes Applicant intends to perform his duties with "utmost integrity and diligence," and considers Applicant worthy of the security clearance he has held for many years. (AE F.) He was "a bit surprised" that the concerns about Applicant's security clearance eligibility involve a failure to comply with the rules and regulations for handling protected information. In his experience, Applicant has always been open and honest, "a man of character and upstanding moral values." He considers Applicant "conscientious almost to a fault." Applicant did not share with him the details concerning "perhaps mishandling of classified information." (Tr. 73-75, 77.)

Policies

The U.S. Supreme Court has recognized the substantial discretion the Executive Branch has in regulating access to information pertaining to national security, emphasizing that "no one has a 'right' to a security clearance." *Department of the Navy v. Egan*, 484 U.S. 518, 528 (1988). When evaluating an applicant's suitability for a security clearance, the administrative judge must consider the adjudicative guidelines. In addition to brief introductory explanations for each guideline, the adjudicative guidelines list potentially disqualifying conditions and mitigating conditions, which are required to be considered in evaluating an applicant's eligibility for access to classified information. These guidelines are not inflexible rules of law. Instead, recognizing the complexities of human behavior, these guidelines are applied in conjunction with the factors listed in the adjudicative process. The administrative judge's overall adjudicative goal is a fair, impartial, and commonsense decision. According to AG ¶ 2(a), the entire process is a conscientious scrutiny of a number of variables known as the "whole-person concept." The administrative judge must consider all available, reliable information about the person, past and present, favorable and unfavorable, in making a decision.

The protection of the national security is the paramount consideration. AG ¶ 2(b) requires that "[a]ny doubt concerning personnel being considered for national security eligibility will be resolved in favor of the national security." In reaching this decision, I have drawn only those conclusions that are reasonable, logical, and based on the evidence contained in the record. Under Directive ¶ E3.1.14, the Government must present evidence to establish controverted facts alleged in the SOR. Under Directive ¶ E3.1.15, the applicant is responsible for presenting "witnesses and other evidence to rebut, explain, extenuate, or mitigate facts admitted by applicant or proven by Department Counsel. . . ." The applicant has the ultimate burden of persuasion to obtain a favorable security decision.

A person who seeks access to classified information enters into a fiduciary relationship with the Government predicated upon trust and confidence. This relationship transcends normal duty hours and endures throughout off-duty hours. The Government reposes a high degree of trust and confidence in individuals to whom it grants access to classified information. Decisions include, by necessity, consideration of

the possible risk that the applicant may deliberately or inadvertently fail to safeguard classified information. Such decisions entail a certain degree of legally permissible extrapolation as to potential, rather than actual, risk of compromise of classified information. Section 7 of Executive Order 10865 provides that decisions shall be "in terms of the national interest and shall in no sense be a determination as to the loyalty of the applicant concerned." *See also* EO 12968, Section 3.1(b) (listing multiple prerequisites for access to classified or sensitive information).

Analysis

Guideline K, Handling Protected Information

The security concern for handling protected information is articulated in AG ¶ 33:

> Deliberate or negligent failure to comply with rules and regulations for handling protected information—which includes classified and other sensitive government information, and proprietary information—raises doubt about an individual's trustworthiness, judgment, reliability, or willingness and ability to safeguard such information, and is a serious security concern.

As a defense-contractor employee with a Secret clearance, Applicant is required to comply with the policies and procedures of the DOD 5220.22-M, *National Industrial Security Program Operating Manual* (NISPOM), which specifies the baseline standards for the protection of classified information released or disclosed to industry in connection with classified contracts. Under ¶ 5-100 of the NISPOM, individuals are responsible for safeguarding classified information entrusted to them. Applicant was found culpable by his employer of committing five separate security violations between November 2009 and November 2015. Neither Applicant's employer nor the SOR cited the NISPOM or company security policies implementing the NISPOM which Applicant violated, but he does not dispute the following security infractions.

In November 2009, he sent an email containing classified Secret technical data (a classified parameter) via his employer's unclassified computer network. While there is no indication that the recipient was unauthorized to receive the information, Applicant as a general user is accountable for complying with information system security requirements under ¶¶ 8-105 and 8-307, including maintaining system security policies. He failed to properly safeguard Secret information and caused spillage onto an unclassified network. Moreover, NISPOM ¶ 4-210 requires that electronically transmitted messages be marked to the classification level of the information in the document, and there is no indication that the email was appropriately marked.

In August 2012, Applicant neglected to properly lock a safe containing classified information in his work area. Under ¶ 5-308 of the NISPOM, security containers are to be kept locked when not under the direct supervision of an authorized person entrusted with the contents.

In October 2012, Applicant placed classified FGI on an information system approved for Secret/NOFORN but not for FGI. The affected program elected in remediation to upgrade the server to Secret/NOFORN/FGI. NISPOM ¶ 10-306 specifies that FGI shall be stored and controlled in a manner that will avoid commingling with other material.

In March 2015, Applicant left a set of working papers classified Secret out on his desk, which was located inside a closed work area not approved for open storage. He failed to properly store the Secret information in a GSA-approved security container, an approved vault, or an approved closed area as required under AG ¶ 5-303 of the NISPOM.

In November 2015, Applicant drafted a classified email on his unclassified computer, which caused contamination of the local area network. Under ¶ 8-100 of the NISPOM, an information security system used to capture, create, store, process or distribute classified information must be properly managed to protect against unauthorized disclosure of classified information, loss of data integrity to ensure the availability of the data and the system. However, the evidence does not establish that Applicant sent the email as alleged in the SOR.[5]

During interviews with OPM investigators and in his response to interrogatories, Applicant mentioned two other security issues. He indicated that he had brought his cell phone into a closed work area on two consecutive days. Although inadvertent, he knew that it was a violation and did not timely self-report his security violation. Applicant also discussed an episode in approximately 2011 where he entered onto an unclassified system a document containing frequency information from which classified information could be discerned. When the incident was detected in February 2014, the affected systems were cleansed. There is no evidence that Applicant was disciplined for the incident, and because neither the cell phone violation nor the system network violations were alleged, they cannot be considered as bases for disqualification. They are relevant

[5] Applicant admits that he committed a security violation in the incident by entering classified information on an unclassified system, but denies sending the email because he recognized his error. SOR ¶ 1.e alleges a violation in that he sent the email containing classified information, and in that regard the pleading is defective. The Appeal Board has held that administrative pleadings are not judged by the strict standards of a criminal indictment and that they should be liberally construed. In ISCR 12-11375, decided on June 17, 2016, citing ISCR Case No. 99-0554 at 4 (July 24, 2000)(other citations omitted), the Appeal Board stated in part:

> The purpose of an SOR is to give an applicant advance notice of the allegations against him or her so that the applicant has a reasonable opportunity to respond to them. . . . In assessing the sufficiency of an SOR, it is necessary to balance the need for fair notice to an applicant against the need to avoid transforming the SOR pleading into a game of wits in which a minor or technical misstep is decisive. . . . As long as there is fair notice to the affected party and the affected party has a reasonable opportunity to respond a case should be adjudicated on the merits of relevant issues and not concerned with pleading niceties.

Applicant clearly knew which violation was covered in SOR ¶ 1.e.

for other purposes, such as assessing whether a mitigating condition is applicable and for the whole-person evaluation.

Applicant violated security procedures in several different aspects. Disqualifying condition AG ¶ 34(c), "loading, drafting, editing, modifying, storing, transmitting, or otherwise handling protected information, including images, on any unauthorized equipment or medium," is established by Applicant sending Secret data on an unclassified network in November 2009; by him placing FGI classified information on a Secret/NOFORN classified information system not approved for FGI in October 2012; and by him drafting an email containing Secret information on his unclassified system in November 2015. AG ¶ 34(g), "any failure to comply with rules for the protection of classified or sensitive information," is clearly established by those violations and by his failures to properly secure a classified storage container in August 2012, and Secret working papers in March 2015. Common to his security violations is a lack of due diligence with regard to carrying out his security responsibilities despite security re-training. AG ¶ 34(h), "negligence or lax security practices that persist despite counseling by management," also applies. Whether due to overconfidence in his ability to determine classification, to being in a rush, to workload, to time pressures, to not taking his security responsibilities seriously enough, or most likely to a combination of these factors, five security violations in six years constitute a relatively recent pattern of negligence.

Security violations are one of the strongest possible reasons for denying or revoking access to classified information, as they raise very serious questions about an applicant's suitability for access to classified information. Once it is established that an applicant has committed a security violation, he or she has a very heavy burden of demonstrating that he or she should be entrusted with classified information. Because security violations strike at the very heart of the industrial security program, an administrative judge must give any claims of reform and rehabilitation strict scrutiny. *See* ISCR Case No. 03-26888 (App. Bd. Oct. 5, 2006).The frequency and duration of the security violations are aggravating factors. ISCR Case No. 97-0435 at 5 (App. Bd. July 14, 1998).

Under Appeal Board precedent, Applicant has a heavy burden to establish mitigation. Applicant's pattern of security violations between November 2009 and November 2015 is difficult to fully mitigate under AG ¶ 35(a), even if it may reasonably be considered infrequent in light of his many years of holding a DOD clearance without any security violations or infractions. AG ¶ 35(a) provides:

> (a) so much time has elapsed since the behavior, or it 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.

Applicant showed some mitigation under AG ¶ 35(b), "the individual responded favorably to counseling or remedial security training and now demonstrates a positive

attitude toward the discharge of security responsibilities," by recognizing his November 2015 computer system and LAN contamination violation and not sending the email, and by self-reporting his violation to his security officials. He has minimized the risk of leaving classified papers unattended by placing a sign on the floor near his door as a reminder when working with classified material. In the past year or so, he removed himself as a classification reviewer and from access to the classified storage container in his office area. He has consulted with a subject-matter expert when he has questions concerning classification. Applicant's employer took other measures, such as removing Applicant's trusted download privilege and limiting him to a 40-hour work week. These procedures are likely to reduce the risk of recurrence of security violations, but only if they are followed. What is unknown is to the extent to which Applicant has put these steps into practice in the last two years. He testified that he generally tries not to create classified working papers any longer and that he has sought advice from a subject-matter expert. There is no corroboration from his employer attesting that he has exhibited a more responsible attitude toward his security obligations. However, there is no evidence that Applicant has committed any security infractions in the last two years.

Yet, some concerns persist about whether Applicant can be counted on to comply with security practices and procedures. He contends that none of his violations were deliberate. Two of the five violations were found by his employer to have been inadvertent. It is easy to see how he could have accidentally failed to spin the lock on the classified container in August 2012 and left a set of Secret working papers on his desk in March 2015, especially if the documents were in a manila folder. Applicant was negligent in not checking the headers and footers of the Excel document for FGI in October 2012. His other violations were in some measure deliberate. Given that Applicant possessed a security clearance for decades, was a classification reviewer, and held a trusted download position, he knew that Secret information was not to be included in an email sent on an unclassified network in November 2009. At a minimum, he should have checked the classification guide or other security references, such as the NISPOM, if he had any questions before sending out the email. Applicant admitted that the parameter that he placed in his email in November 2015 was clearly classified per the classification guide. Applicant did not report some of his security violations to his employer in a timely manner. Applicant testified that he now realizes the importance of being open and transparent to avoid regarding security infractions as "no big deal." Applicant has received annual security refresher training for years so it should not have taken the possible loss of his security-clearance eligibility for him to realize the importance of complying with all his security obligations.

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 his conduct and all relevant circumstances in light of the nine adjudicative process factors listed at AG ¶ 2(d).[6] Some of the factors in AG ¶ 2(d) were addressed under Guideline K, but some warrant additional comment.

[6] The factors under AG ¶ 2(d) are as follows:

Applicant's counsel would have the Government consider Applicant's security violations as of minimal concern ("de minimis") when viewed in light of Applicant's unblemished security record for previous decades. His long history of security compliance leads one to question whether his relatively recent violations were situational, such as due to work pressures, or were borne of a complacency toward discharge of his security responsibilities developed over years of familiarity handling classified information. In the latter case, a change of circumstances, such as limiting work hours and security duties, would not necessarily preclude a recurrence. Applicant did not think that his security violations were serious enough to disclose on his SF 86. In April 2017, Applicant attributed his security violations in part to him not taking his security obligations seriously enough. This attitude is not easily reconcilable with his reputation among his friends for exhibiting attentiveness to detail and being "conscientious almost to a fault." Applicant's character reference information is favorable, but his friends were not fully aware of the Government's security concerns.

It is well settled that once a concern arises regarding an applicant's security clearance eligibility, there is a strong presumption against the grant or renewal of a security clearance. *See Dorfmont v. Brown*, 913 F. 2d 1399, 1401 (9th Cir. 1990). Perhaps with more time and proven attentiveness to his security obligations, Applicant may be able to demonstrate that he can be trusted to responsibly handle classified information. Based on the facts and circumstances before me, for the reasons noted above, I do not find it clearly consistent with the national interest to continue Applicant's security clearance eligibility at this time.

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:	AGAINST APPLICANT
Subparagraphs 1.a-1.e:	Against Applicant

---

(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.

Conclusion

In light of all of the circumstances presented by the record in this case, it is not clearly consistent with the national interest to grant or continue Applicant eligibility for a security clearance. Eligibility for access to classified information is denied.

_____
Elizabeth M. Matchinski
Administrative Judge