DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:)
)
) ISCR Case No. 17-03588
)
Applicant for Security Clearance)

Appearances

For Government: Nicholas T. Temple, Esq., Department Counsel
For Applicant: *Pro se*

12/11/2018

____

Decision

____

MATCHINSKI, Elizabeth M., Administrative Judge:

Applicant inadvertently violated security policies and procedures in May 1995 when he inserted in a memorandum technical information from which an engineer with knowledge could determine classified data. He caused spills of classified data in March 2006, March 2013, August 2014, and November 2016, by emailing files with classified information to cleared co-workers via his company's unclassified network. Applicant was well-intentioned, but the pattern of similar security incidents casts doubt about his security worthiness. Clearance is denied.

Statement of the Case

On January 19, 2018, 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 *National Security Adjudicative Guidelines for Determining Eligibility for Access to Classified Information or Eligibility to Hold a Sensitive Position* (AG) effective within the DOD on June 8, 2017.

On January 22, 2018, Applicant answered the SOR allegations and requested a hearing before an administrative judge from the Defense Office of Hearings and Appeals (DOHA). On April 18, 2018, 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 August 6, 2018, I scheduled a hearing for September 18, 2018.

I convened the hearing as scheduled. Seventeen Government exhibits (GEs 1-17) were admitted in evidence, which included reports of administrative inquiries into security violations and written reprimands about which Applicant expressed some concerns and objections. Two Applicant exhibits (AEs A-B) were admitted into evidence. Applicant, his spouse, and his son-in-law testified, as reflected in a transcript (Tr.) received on October 3, 2018.

Summary of SOR Allegations

The SOR alleges under Guideline K that Applicant risked a data spill by directing his secretary to type a memorandum containing protected information on an unclassified computer in approximately May 1995, and that he did not inform security officials of the potential data spill (SOR ¶ 1.a). Applicant is also alleged under Guideline K to have improperly emailed a file containing protected information on an unclassified network causing a data spill in about 1998 (SOR ¶ 1.b), March 2006 (SOR ¶ 1.c), April 2013 (SOR ¶ 1.d), August 2014 (SOR ¶ 1.e), and November 2016 (SOR ¶ 1.f).

In a detailed response, Applicant denied that he deliberately violated security regulations in May 1995 because the Security Classification Guide (SCG) did not specify that the technical information in his memo was classified. He acknowledged that a chief systems engineer determined that the information could be used to figure out frequency data, which was classified. Applicant admitted the security violations in 1998 (SOR ¶ 1.b) and March 2006 (SOR ¶ 1.c), but stated that he does not clearly recall the violations. Although Applicant was alleged to have signed a letter acknowledging the April 2013 security violation (SOR ¶ 1.d), he denied the violation on the basis that the protected information in his email was not classified in the SCG at the time. It was only after he sent the email that a decision was made to treat the information as classified. Applicant also denied the August 2014 violation (SOR ¶ 1.e), explaining that he had been asked for his input on a proposal. He cropped figures to remove classified values, but in pasting the data, he used a destination style, not knowing that it would cause the classified values to reappear. He denied any intention to share protected information. Applicant denied the November 2016 violation (SOR ¶ 1.f), and indicated that he was asked to resolve an urgent problem within 24 hours and used an Excel document provided by a company engineer years ago that unbeknownst to him was classified. He inadvertently included classified information in a PowerPoint document, which led security officials to seize his work computer. All of the violations involved dissemination to authorized persons. (Answer.)

Findings of Fact

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

Applicant is a 70-year-old senior principal engineering fellow with a defense contractor. He and his spouse are naturalized U.S. citizens who met and married in the United States. They had a daughter in 1977, who lived five years. They have two sets of twin daughters born in 1978 and in 1986, who are all married and successful college graduates. Applicant and his spouse have nine grandchildren. (GEs 1-2; Tr. 15, 64, 111, 115-120.)

Applicant has worked for his defense-contractor employer (company X) most recently since March 1987. He previously worked for the company from 1979 to 1981. He has been at his current job location since 2015. (GE 1; Tr. 64-65.) He has a bachelor's degree earned in 1971, a master's degree in electrical engineering awarded in 1975, and a doctorate degree awarded in June 1979. Applicant was initially granted a DOD security clearance in 1979. His clearance was renewed in April 1987 for his work with company X, and he has held a Secret or Top Secret security clearance since then. (GEs 1-4.) His security clearance eligibility was last renewed in May 2015, when he was granted a Secret clearance. (GE 12.)

Applicant developed considerable technical expertise in his field during his more than 30 years with his employer. He holds 21 U.S. patents with some work colleagues, including five patents granted since January 2016, and he has published 39 papers. (Answer; AE A; Tr. 16-17, 60.) He executed a classified information Non-Disclosure Agreement (Standard Form 312) with his employer on December 7, 1998. He had annual DOD security refresher briefings about his security responsibilities from at least 2006 to as recently as January 2, 2018, as required by his employer,[1] and annual

[1] The Government entered in evidence company X's security-indoctrination briefing as of 2016. (GE 15.) Individuals are briefed on their responsibility to report to security any issues covered by the 13 adjudicative standards, including use of information technology systems. In that regard, employees are informed to report any security violations that come to their attention, such as when "classified information is processed, manipulated, or stored on a computer not approved for classified processing (i.e., data spill)." Those briefed are also informed of the National Industrial Security Program Operating Manual (NISPOM), and are specifically advised that classified information must be accessed only by individuals with an appropriate level of clearance and a valid need-to-know; kept under the control or guarded by an authorized person or stored in a locked security container, vault, secure room or secured area and not left unattended; discussed in an area authorized for classified information or on a secure telephone; marked appropriately; transmitted via secure communications methods; processed on a computer or other equipment approved by the government; and destroyed by approved methods. They are informed that employees with derivative classification authority are required to complete Derivative Classifier training every two years. About classified information systems processing, they are briefed that DOD classified information may only be processed on information systems approved and accredited by the cognizant security authority; that the use of personal laptops or other devices is prohibited; and that any classified

classified information system user briefings from 2013 through 2017.[2] Applicant was also given closed-area briefings in April 2009, September 2013, and November 2016.[3] He completed derivative classification briefings every two years between January 2014 and January 2018, which was required by his employer. (GEs 13, 17; Tr. 67-68, 76.) The information in the briefings he had over the years remained substantially the same throughout his tenure at company X. (Tr. 68.) Applicant's present desire and focus is to mentor younger engineers to boost his employer's technical contributions to the U.S. national interest. (Tr. 59.) He has not previously had his security clearance eligibility questioned despite some security violations on his record. The salient details of those violations are as follows.

May 1995 violation (SOR ¶ 1.a)

While working as a principal engineer with a secret clearance in May 1995, Applicant created a six-page memorandum that was typed by his secretary in her office using a dedicated computer that was not cleared for classified processing. The secretary held a Secret clearance. The document, which was distributed to ten employees of company X, was thought to be unclassified by Applicant based on his interpretation of the SCG dated June 1992. Applicant was then the leading analyst on the system, and he was asked to write a technical memorandum by the chief engineer, who planned to use the memorandum to explain the system issue to a customer. (Tr. 20.) On review of the memorandum in June 1995, a scientist on the program advised Applicant that he thought the memorandum should be classified at the Secret level due to the possibility that someone with sufficient knowledge could derive Secret information from the technical data in the memorandum. At Applicant's direction, his secretary

information processing on a non-accredited system must be reported immediately to the facility security officer or information systems security manager (ISSM). About computer data spills, which occurs when classified data "is accidentally processed, released or received on an unclassified PC (or associated devices), network or voice mail," cleared employees are informed about the possible damage caused by data spills, costs, and consequences for the offender. Employees are specifically advised to notify security immediately in the case of a data spill and to know the SCG so as to avoid a data spill.

[2] Available documentation of company X's annual cybersecurity awareness training (GE 16) is dated May 2018. All users of a classified information system are required to read and understand the company's security plan and acknowledge their responsibilities. Current cybersecurity awareness training informs cleared company X employees that all media and systems must be conspicuously marked with the classification level or labeled as unclassified, and that unclassified hardware cannot be used for classified purposes or as peripheral equipment on a classified information system at any time. Guidance in preventing data spills reminds the briefed employee that data by itself maybe unclassified but when combined with other data may become classified and to ask a subject matter expert if unclear. Information assurance personnel are to be notified when there is a classified data spill. The annual cybersecurity awareness training also reminds those employees who anticipate creating derivatively classified material about the requirement to take Derivative Classifier training every two years. Applicant acknowledged that he received similar briefings before 2018. (Tr. 67.)

[3] Available closed area-briefing documentation (GE 14) was published in 2016 and revised on June 21, 2018. Under that guidance, closed areas are established to protect information systems processing classified information and or classified information, which, due to their size and nature, cannot be stored in a secured container. The briefing provides that closed areas are generally not approved for open storage of classified material.

retrieved all of the distributed copies that she could before she left the company's employment in late June 1995. The memorandum was taken to the classified publications area to have the classification marking changed from unclassified to Secret. Applicant did not report the incident to his security office. (GE 3; Tr. 71-73.)

In early August 1995, a Defense Investigative Service industrial security representative (IS representative) conducted an inspection in the publications area at the facility. She discovered two copies of the memorandum in a classified container that was assigned to an employee with a Secret clearance. One copy was marked Secret and the other was marked unclassified. At the request of the IS representative, a company X security manager initiated an administrative inquiry (AI) to determine the reason for the difference in the classification of the memoranda. During the inquiry, Applicant admitted to the security manager that he had his then secretary type the memorandum on her unclassified computer. He marked the document unclassified based on his interpretation of the SCG, which he asserted did not identify the data as classified. The security manager removed the affected computer and brought it to the document control station. Security then contacted the employees who had received the initial memorandum. All of the employees held at least a Secret clearance. Six of the copies were recovered. The other four copies, which were not marked, were discarded in company refuse. In reporting his findings of the AI in September 1995, the security manager opined that because some copies of the document had been discarded, the possibility of compromise could not be ruled out. However, he also indicated that the classified data that could have been derived from the parameters in Applicant's memorandum was no longer classified as of mid-August 1995 based on the program's security guide. Applicant was found culpable for the violation. He was issued a reprimand and re-briefed on his responsibility to promptly notify the security office of any future similar incidents. (GE 3; Tr. 20-21, 74.)

In early October 1995, the IS representative informed the security manager that she was concerned about the failure of employees to notify their security officials when the classification issue was presented, and about the inadequacy of the classification review process before a document is released. Noting that several instances of classification error had occurred with respect to the particular program, she recommended that the employees on the program be briefed on their reporting requirements with respect to classification errors, security violations, and computer security. The IS representative noted that Applicant had his memorandum reviewed as required, and despite that fact, it was released as unclassified. Moreover, she noted that none of the ten employees contacted by the secretary to retrieve the copies reported the incident to security personnel. The IS representative notified the Defense Industrial Security Office of Applicant's culpability for the violation. (GE 3.)

1998 violation (SOR ¶ 1.b)

The SOR alleges that Applicant caused a data spill by improperly emailing a file containing protected information via an unclassified network in about 1998, and that Applicant's supervisor advised him that he had committed a security violation. Applicant admitted the allegation when he responded to the SOR, but he also indicated that he had no recall of the incident. The allegation may well stem from Applicant's voluntary disclosure during his October 2013 subject interview that he had a committed a security violation prior to the 2013 violation. He indicated that it occurred approximately 15 years ago, which would have been 1998 as of his 2013 interview. He explained that he sent an email to a chief engineer, which included a Word document containing classified information, but there was no clear classification guidance. (GE 2.) Applicant appears to have been discussing the 2006 violation, which involved the same named engineer. At his hearing, Applicant reiterated that he had no recollection of any security incident in 1998. (Tr. 77.) The evidence falls short of establishing that Applicant violated security practices and procedures in 1998.

March 2006 violation (SOR ¶ 1.c)

In mid-March 2006, Applicant and a colleague at company X prepared a PowerPoint presentation for a symposium to be held in May 2006 on a design they had created. Applicant marked up a hard copy of the presentation by changing one word on the title page. The word was considered classified at the Secret level. Applicant's colleague made the change to an electronic copy of the PowerPoint presentation saved on his laptop before emailing the updated PowerPoint presentation to Applicant. Six days later, Applicant sent emails to his colleague and five other co-workers with the contaminated PowerPoint presentation attached. One of the co-workers who had read the attachment notified the program security manager of the security violation. A company X information systems security manager (ISSM) immediately conducted an AI. Efforts were then taken to delete the emails and wipe the contaminated file from the affected computer drives. Email server backup tapes were removed and taken to document control at another company X facility. Applicant had printed the document to a printer in another building and had stored it in his locked office. The first page was removed and turned into document control. As required by ¶¶ 1-303 and 8-100 of the NISPOM, the ISSM notified the Defense Security Service (DSS) of the results of the AI. The ISSM concluded that compromise had occurred because Secret information resided on an unclassified email server and on unclassified computers for ten days. Applicant was found culpable of an inadvertent security violation for transmitting an email that contained classified information. He was issued a written reprimand per company X's security standards and procedures for a first non-deliberate security violation in a 12-month period.[4] He was advised that any further violation within the next 12 months would result in further disciplinary action ranging from five days unpaid suspension to termination of employment. He also re-briefed about his responsibilities to be knowledgeable of the procedures for safeguarding classified information. After the

[4] Under its security enterprise standard, company X has a graduated scale of disciplinary action for a failure to adhere to established security rules and regulations. A written reprimand is issued for a first offense. For a second offense within a 12-month period, the discipline is suspension without pay for one to five days. For a third offense within a 12-month period, the discipline is suspension without pay for six to ten days up to and including employment termination. (GE 15.)

incident, company X realized that the work on the specific project needed to be completed in a closed area. (GEs 4-5; Tr. 81-83, 85.)

On August 12, 2009, Applicant was interviewed by an authorized investigator for the Office of Personnel Management (OPM). He volunteered that he had been cited for the March 2006 security violation for accidentally transmitting an email that contained information that was not classified by the DOD but was considered classified information by the chief engineer on the project. He indicated that he had received a written warning, but it was an internal violation. When interviewed by an OPM investigator in October 2013, Applicant explained about the incident that it was not clear in the SCG that the information was classified. He was re-interviewed in November 2013 for further details about that incident and about the security violation in 2013. He explained about the 2006 incident that he sent the email not knowing that it contained classified information. (GE 2.) Applicant testified at his hearing that the word he added became classified in context, *i.e.*, put together with the program name. Applicant now understands that he should have had the document reviewed by the government program officer before dissemination. He asserted he is currently following that practice. (Tr. 80-81.)

April 2013 violation (SOR ¶ 1.d)[5]

On March 18, 2013, Applicant sent an unsecure email with an attached PowerPoint file containing data relating to three classified programs to four company X employees at two different facilities. The next day, one of the recipients, an electrical engineering manager with a Top Secret clearance, notified company X security that there was a possible issue with an email received from Applicant. On notification, the attached file was reviewed for classification by the manager and a subject matter expert with a Secret clearance. The aggregation of the data with the programs' names made the PowerPoint classified to the Secret level. Cleanup actions were taken, including delivering the email server and file-share backup tapes to document control. Applicant showed his ISSM where the contaminated file was located on his hard drive, and it was removed. He admitted that he had printed the document, and the hard drive for the affected printer was removed for destruction. In reporting the results of his AI to the DSS in accord with ¶¶ 1-303 and 8-100 of the NISPOM, a security manager concluded that a loss of classified information was assumed based on the fact that classified information resided on an unsecured network for four days. Applicant was identified as the culpable employee. On April 8, 2013, he was issued a written warning for inadvertently publishing information that was determined to be classified onto unclassified systems. Applicant was advised that, as an engineer who develops or formulates data in support of classified programs, it was vital for him to understand the customer's SCG. In late June 2017, the DOD CAF was notified of Applicant's security violation. (GEs 6-8; Tr. 83-84.) Applicant removed himself from working on the program involving co-sites to minimize the risk of another data spill. (Tr. 86-87.)

[5] The AI's findings indicate that the violation occurred on March 18, 2013, and not in April 2013. (GE 6.)

During his October 2013 interview with an OPM investigator, Applicant volunteered about the incident that he had performed an analysis of a system for a client as a favor. He emailed on an unclassified network two files consisting of a PowerPoint presentation and a spreadsheet to some company X employees with security clearance. He stated that because he emailed the files together, they were considered classified by aggregation. Applicant indicated that he cooperated with the company's investigation and acknowledged in writing his violation of a security policy. Applicant denied receiving any remedial security education as a result of the incident. He kept his same job assignment but was told that there would be a serious penalty, such as a reduction in salary, for another security infraction. When re-interviewed in November 2013, Applicant explained that he was working on a proposal and not an established program, so there was no closed room where he could handle the classified data. He did not realize that by sending the two files at the same time, the data when aggregated became classified. Applicant explained to an OPM investigator in August 2017 that the chief engineer had not properly briefed him about the project. He learned from the incident to ask those working on the project to review information for its classification level before any dissemination, especially for a proposal that does not have a SCG. Applicant also realized that he should have met with the chief engineer in person to discuss the solution rather than send an email. (GE 2.) Applicant asserts that he could not have known that by aggregating the data about three programs it became classified, and that the systems engineer in charge of implementation bears some responsibility for not giving him proper guidance about the classification issue.[6] (Tr. 43-44.)

August 2014 violation (SOR ¶ 1.e)

On August 6, 2014, Applicant sent an email with a PowerPoint attachment to two work colleagues with Secret clearances. He sent a separate email containing a different version of the PowerPoint file to a recipient of the first email and to two additional cleared colleagues. Under the SCG for the program at issue, the PowerPoint contained data classified at the Secret level. The employee that received the two emails notified his security manager, and corrective action was taken immediately to secure printed copies of the PowerPoint presentation and remove and wipe the affected computers and hard drives. Applicant was removed from the affected program and issued a written warning letter in which he was advised that since the Secret data was sent over the Internet, it was deemed a compromise of classified information. As required by ¶¶ 1-303 and 8-100 of the NISPOM, DSS was informed of the violation in a report dated September 4, 2014. Based on the fact that classified information resided on an unsecured network from August 5, 2014, to August 6, 2014, a company X security manager advised the DSS that it must be assumed that a loss of classified information occurred. Applicant was identified as the culpable individual. (GEs 9-10; Tr. 92-93.)

[6] Applicant provided details of the April 2013 security incident when stating his concerns regarding GE 5, which is the written warning issued to him for a non-deliberate violation in March 2006. He provided details of the August 2014 security incident when stating his concerns about GE 6, which is his employer's findings of the April 2013 violation.

When interviewed by an OPM investigator in August 2017, Applicant explained that he created a scale diagram to solve a problem related to a company X proposal. Applicant knew that the numbers on the side of the scale were classified, and so he cropped the numbers before sending a graph diagram by email to other company X employees. One of the recipients noticed that if he clicked the diagram, the picture reverted to the previous version containing Secret information. Applicant acknowledged he was at fault for the violation, which he attributed to rushing to send the solution while working on three projects simultaneously. There was no SCG for Applicant to review because the project was in the proposal phase. Applicant now understands that he should have double-checked the diagram before emailing it and that he should have sent the email via company X's classified network. Applicant related that he has taken corrective action to preclude a recurrence by having those working on a project to confirm the security classification level. (GE 2.) He also has a colleague review his emails before sending them, and any attachments are now in PDF format. (Tr. 91-92.) Applicant attributes the violation to him not knowing that the full image with the classified information was recoverable. He asserts that company X should have provided him access to a closed area to process the classified image. (Tr. 45-46, 87-90.)

November 2016 violation (SOR ¶ 1.f)

In response to a company X customer inquiry, Applicant prepared a PowerPoint presentation diagnosing a technical issue for a deployed system. He included technical specifications that were classified Confidential under the program's SCG. Applicant obtained the technical specifications from an Excel spreadsheet provided to him in 2009 by a co-worker who then separated from company X in 2012.[7] Applicant had saved the spreadsheet on his work computer. In early November 2016, Applicant emailed the PowerPoint presentation to an engineering fellow with a Secret clearance at his facility and to two company X employees at another facility: a senior principal mechanical engineer with a Secret clearance who reported the incident to her ISSM and an engineering fellow with a Top Secret clearance, who as a subject matter expert confirmed the classification level. ISSMs at both facilities coordinated the collection and cleanup of impacted assets in accord with the company's data spill response guide. Applicant was deemed responsible for the violation. In reporting the violation to the DSS in accord with ¶ 1-303 of the NISPOM, the ISSM at Applicant's facility concluded that classified information was compromised because classified information had been included on an information system not approved for classified processing. (GEs 11-12.)

An incident report was filed with the DOD CAF about Applicant's security violation. (GE 12.) In late November 2016, company X filed a subsequent incident report notifying the DOD CAF that the November 2016 incident was Applicant's fourth security violation since 2006. In December 2016, the company notified the DOD CAF that the Excel spreadsheet containing classified specifications had resided on Applicant's

[7] There is no indication that the spreadsheet was conspicuously marked with its classification level, although the technical information was identified as classified in the program's SCG.

unclassified computer since 2009, and the contaminated email was on unclassified email servers and recipient systems for approximately 24 hours. Therefore, it was determined that a loss of classified information had occurred. Applicant was counseled that it was critical to periodically review files for classified information before dissemination. (GE 12.)

Applicant explained to an OPM investigator in August 2017 that his supervisor needed him to troubleshoot a problem on an emergency basis. Applicant was his company's subject matter expert on a component. Applicant created a PowerPoint slide presentation outlining the steps he took to resolve the problem and sent it by email to some company X employees. The following morning, he was told that he had included "Secret" information in the PowerPoint presentation.[8] Applicant explained that the classified information consisted of an item that was deemed classified by the project's chief engineer. Applicant denied knowing that the new number was classified. He asserted to company X security personnel that he should have been provided the SCG because he was not privy to all of the classification specifications. Applicant detailed his discipline for the violation, which consisted of one week of suspension without pay, which he served in February 2017; inability for a pay increase in 2017; and a reduction by half of his 2016 bonus. He was required to complete a security clearance application (SF 86) immediately, which prompted the background investigation. (GE 2; Tr. 97-98.)

About lessons learned, Applicant admitted that he should have asked for the project's SCG before working on the problem and emailing the PowerPoint. Regarding corrective actions for the future, he expressed his intention to document his work in hardcopy first for the chief engineer to determine its classification level; to not send any electronic copy without first having it reviewed; and to take more time to review the SCG rather than rush to show that he had solved a problem. Applicant acknowledged his culpability for the violation in that he was negligent in not reviewing the SCG on the project. He stated that he does not believe classified information was compromised because the PowerPoint was sent only to company X employees and the information stayed within company X's computer systems network. Applicant displayed remorse over his violations and appeared motivated to follow proper security protocols in the future because he plans on retiring in the next few years and does not want to jeopardize his career or future retirement benefits. (GE 2.) Applicant accepts responsibility for the violation. He had received the Excel spreadsheet in an unclassified format and had not known that the Excel spreadsheet contained classified information. (Tr. 48, 93-97.) After the incident, he obtained the SCG for the program so that he could use it as guidance in performing maintenance to modernize the system. (Tr. 96.)

Applicant attributes all of his security violations to the "gray environment" when the projects were in the development stage, and the SCG was not clearly defined. He lacked any deliberate intention to compromise classified information, which was disseminated through emails to company X employees authorized to receive the information. He asserts that the lead system engineers on the projects and the DOD bear some responsibility for his security violations in that he should have been provided

[8] The report of the AI indicates that the material was classified, but at the Confidential level. (GE 11.)

a clear and updated SCG. He submits that in all cases, he was the only company X employee who fully understood the system's operation, which placed pressure on him to resolve the issues quickly and report progress to lead systems engineers outside of his department. (Tr. 17-19, 42.)

Applicant has continued to provide timely and effective solutions to a wide assortment of complex problems for his employer. He is highly respected by systems engineers and his peers at work. (AE B.) He is currently working on a program to improve U.S. defense capability and plans to retire in two years. (Tr. 59, 61.) He mentors two employees who use his mathematical model to process classified data in a closed area. (Tr. 71, 99-100.) He has not committed any security violations since November 2016. (Tr. 98.)

Applicant has an active role in his church's leadership. He became an elder in 1999, has mentored church members looking for employment, and is involved in a search for a new pastor. He and his spouse counsel couples with troubled marriages and parents with troubled children. (Tr. 16, 107, 111-112.)

One of Applicant's sons-in-law testified for him. This son-in-law is a licensed attorney who has stayed at home to care for his and his spouse's three children since 2010. (Tr. 104.) Based on his review of the SOR and discussions with Applicant, he believes the incidents occurred when Applicant was working on projects outside of his group where he did not fully understand the rules. He considers Applicant "an upright man of integrity who has noble intentions and always tries to do the right thing." (Tr. 106-107.) Applicant has always been generous and fair with his time and attention. (Tr. 110-111.)

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(c), 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 access to classified information will be resolved in favor of 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.

In May 1995, Applicant inadvertently violated those security procedures that require processing of classified information on approved equipment and marking of classified information with its appropriate classification level. He created a technical memorandum, which he marked and treated as unclassified based on his interpretation of the SCG. He had a secretary type the memorandum on her unclassified computer, and he disseminated ten copies internally to co-workers before learning that the document should have been marked Secret because an engineer with knowledge could ascertain classified data from the information. On being advised that the document should have been treated as Secret, he asked his secretary to retrieve the copies he had disseminated, but he did not report the incident to security officials. His noncompliance with his reporting obligation may well have led to compromise. Secret information was unprotected until August 1995, when the issue was discovered by a DIS representative during an inspection. Four unmarked copies of his memorandum were apparently discarded as trash. More recently, Applicant caused spills of Secret classified data in March 2006, March 2013, and August 2014, and of Confidential classified data November 2016, when he sent emails with attachments that contained the classified information to other employees on a company information system not approved for classified processing or transmission. In August 2014, he apparently transmitted classified data over the Internet.

Regarding disqualifying condition AG ¶ 34(a), "deliberate or negligent disclosure of protected information to unauthorized persons, including, but not limited to, personal or business contacts, the media, or persons present at seminars, meetings, or conferences," Applicant did not set out to disclose or release classified information to persons unauthorized to receive it. The recipients of his emails containing classified attachments in 2006, 2013, 2014, and 2016 were all cleared employees of company X who were authorized to receive the information. At the same time, compromise cannot be completely ruled out because the classified information was sent as attachment by email on an unapproved computer system. Four copies of his improperly marked as unclassified memorandum in 1995 were not recoverable because they were discarded as ordinary trash.

AG ¶ 34(b), "collecting or storing protected information in any unauthorized location," and AG ¶ 34(c), "loading, drafting, editing, modifying, storing, transmitting, or otherwise handling protected information, including images, on any unauthorized equipment or medium," apply in that Applicant caused classified information to reside on unapproved network systems or computers for varying periods depending on the violation. Regarding the March 2006 violation, Applicant kept a printed copy of the PowerPoint presentation in his locked office. The Excel spreadsheet from which he obtained Confidential technical information for his November 2016 PowerPoint presentation resided from 2009 to November 2016 on Applicant's computer not authorized for classified processing or storage.

AG ¶ 34(g), "any failure to comply with rules for the protection of classified or sensitive information," is clearly established. Moreover, AG ¶ 34(h), "negligence or lax security practices that persist despite counseling by management," applies because of the pattern of data spills between March 2006 and November 2016 that probably could have been avoided had Applicant reviewed the appropriate SCGs or consulted with program experts and engineers about the classification level of the data before transmitting it by email over an unapproved network. He had annual security refresher and cybersecurity awareness security briefings since 2006, which alerted him about data spills and how to avoid them. Moreover, after the March 2006 incident, he was re-briefed about his responsibilities to knowledgeable of and safeguard classified information. After the April 2013 violation, he was advised that, as an engineer who develops or formulates data in support of classified programs, it was vital for him to understand the SCG. He did not have an SCG available for review concerning the data involved in the August 2014 incident, but he admitted that he should have those working on the proposal to review his email and attachment before sending it. He certainly risked a data spill with respect to sending unmarked classified information via the Internet. The failure of a former co-worker to appropriately mark an Excel spreadsheet as classified was a significant factor in Applicant's November 2016 security violation, his fourth in little more than a decade. At the same time, Applicant let his desire to provide a quick solution to the problem dictate his actions. He acknowledges that he should have reviewed the SCG for the program.

Applicant has the burden of mitigating the security concerns raised by his repeated noncompliance with the rules and regulations for handling protected information. Applicant's failure to follow security guidelines on which he was trained since 2006 is difficult to fully mitigate under AG ¶ 35(a), even if it may reasonably be considered infrequent when considering 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.

Albeit belatedly, Applicant exhibits 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." Applicant has removed himself from working on a classified program involving co-site issues involved in the 2013 violation because of the complexity, which he does not feel he can handle. He indicated in August 2017 that he learned from the 2013 incident to have those familiar with the projects review information for its classification level before he makes any dissemination. After the November 2016 incident, he expressed his intention to document his work in hardcopy so that the chief engineer could determine its classification level; to refrain from sending any electronic copy until it is reviewed; and to take more time and care in reviewing the applicable SCG. These are all favorable steps which, if followed, will go a long way toward preventing a recurrence of any security violations similar to those he committed since 2006. He testified, with no evidence to the contrary, that he has not had any security infractions since November 2016. However, Applicant continues to downplay his culpability for the security infractions to the extent that he blames other engineers for not advising him of the security classification and, in some cases, for placing unreasonable expectations on him to solve a problem.

On unfamiliar programs or programs in the proposal stage, he understandably may not have recognized the information as classified, especially when data became classified by aggregation. AG ¶ 35(c), "the security violations were due to improper or inadequate training or unclear instructions," would have some applicability to the May 1995 and April 2013 violations. Applicant was the leading analyst on the system involved in May 1995, but the IS representative who discovered the violation indicated that there had been several classification errors on the program. Applicant had his memorandum reviewed as required, and despite that fact, the memorandum was released as unclassified. Presumably the reviewer did not recognize that the data as classified. The April 2013 violation involved three classified programs, and was at the proposal stage. The August 2014 violation occurred because Applicant did not understand the computer program he used to crop classified numbers from a graph diagram. The technical specifications improperly transmitted in the November 2016 incident were classified Confidential in the SCG. Applicant relied to his detriment on an improperly marked Excel spreadsheet for the data. Even so, as a longtime cleared employee, Applicant can reasonably be held to have understood security practices and procedures and the importance of ensuring that no classified information was divulged improperly. His lack of due care in discharging his security responsibilities cannot completely be explained by inadequate training or instructions.

Applicant's violations were inadvertent, but in each case, they were discovered and reported by someone other than Applicant. Moreover, compromise was assumed in the data spill incidents. AG ¶ 35(d), "the violation was inadvertent, it was promptly reported, there is no evidence of compromise, and it does not suggest a pattern," is not mitigating of the security concerns. Applicant's commission of four serious security violations since 2006 continues to cast some doubt about his ability to handle classified information appropriately.

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).[9]

Applicant's value to his employer and to the national defense effort is undisputed. He holds some 21 patents on systems vital to the Nation's defense. I do not doubt that he has personal integrity. He did not plan to violate security regulations. He held a security clearance for years with only one violation before 2006, but it makes his lack of due diligence in carrying out his security responsibilities in recent years all the more troubling. 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). Based

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

> (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.

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
Subparagraph 1.a:	Against Applicant
Subparagraph 1.b:	For Applicant
Subparagraphs 1.c-1.f:	Against Applicant

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