DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 21-00363
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Gatha Manns, Esq., Department Counsel
For Applicant: Alan V. Edmunds, Esq.

11/25/2022

_____

Decision

_____

PRICE, Eric C., Administrative Judge:

Security concerns under Guideline K (handling protected information) and Guideline E (personal conduct) are not mitigated. Eligibility for access to classified information is denied.

Statement of the Case

On June 30, 2021, the Department of Defense (DoD) issued to Applicant a Statement of Reasons (SOR) detailing security concerns under Guideline K, handling protected information, and Guideline E, personal conduct. The action was taken under Executive Order (EO) 10865, *Safeguarding Classified Information within Industry* (February 20, 1960), as amended; Department of Defense (DOD) Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (January 2, 1992), as amended (Directive); and the adjudicative guidelines (AG) effective within the DOD on June 8, 2017.

On August 16, 2021, Applicant answered the SOR, and requested a hearing before an administrative judge. The case was assigned to me on March 2, 2022. On March 8, 2022, the Defense Office of Hearings and Appeals (DOHA) issued a notice of hearing

scheduling the hearing via video teleconference. I convened the hearing as scheduled on March 24, 2022. During the hearing, Department Counsel offered Government Exhibits (GE) 1 through 7. Applicant testified and offered Applicant Exhibits (AE) A through L. There were no objections, and all exhibits were admitted into evidence. The Government's exhibit list, pre-hearing disclosure letter, and the resume of a Government witness were marked as hearing exhibits (HE) I through III. Applicant's exhibit list was marked as HE IV. DOHA received the hearing transcript (Tr.) on April 8, 2022.

Findings of Fact

After a thorough and careful review of the pleadings, testimony, and exhibits submitted, I make the following findings of fact.

Applicant is 56-years-old. He has been married since 1988 and has two adult children. He received bachelor's and master's degrees in electrical engineering in 1988 and 1994, respectively. He was employed in various positions for a federal contractor from June 1990 to November 2019, and has been employed as a senior system engineer for another federal contractor since November 2019. He supported the same DoD agency for more than 20 years until June 2020. (GE 1, 3; AE C, D, F-H, K, L; Tr. 22-23, 38-39, 54-55)

Applicant has held a security clearance since 1988. He was granted access to a classified DoD IT system in approximately 2005. He was provided email accounts on classified and unclassified DoD IT systems and issued a Government laptop computer. He has received training on information security and the proper handling of classified information, including periodic refresher training. His access to classified information was suspended in June 2020 and his security clearance was suspended in November 2020. (GE 1, 3, 4, 7; AE D; Tr. 12-23, 42, 48, 55-56, 73-74)

From approximately 1999 to March 2020, Applicant maintained a large, comprehensive electronic spreadsheet file (spreadsheet) containing his personal information including commercial account access information, tax and other financial information, medical information, and to-do lists. The spreadsheet included approximately 20 worksheet tabs of information. From approximately 1999 to 2015, he maintained the spreadsheet on an encrypted, personal universal serial bus (USB) drive that he accessed and updated, at home or work, as needed. He reported that in approximately 2015, DoD revised its information security rules and prohibited the introduction of personal USB drives onto DoD IT equipment. From 2015 to 2019, he maintained and routinely transmitted the spreadsheet as an encrypted, password protected file between his DoD and personal email accounts. (GE 2; AE L; Tr. 38-43, 53-58)

From at least 2015 to March 2020, he also maintained protected DoD information in the spreadsheet including safe access information, and personal identification numbers (PINs) for facility access, unclassified and classified IT network access, and for his DoD ID card. The word "Safe" was followed by a six letter passcode which could be converted into a DoD safe's numerical combination. (Tr. 63-64, 69-71; AE L at 1) He maintained the

protected DoD information in a single worksheet tab titled "info" along with passwords for various personal accounts and for his home safe. (Tr. 41) He routinely accessed and revised the spreadsheet to reflect changes in his personal and protected DoD information including the safe's passcode in 2017. (GE 1, 2, 4; AE L; Tr. 40-42, 53-57)

Applicant reported that in 2019, the DoD agency he supported revised their information security rules to prohibit transmission or receipt of encrypted emails between DoD and personal email accounts. He said that in compliance with that policy, he ceased emailing updated versions of the encrypted file from his personal email account to his DoD email account. By March 2020, he reached a point where the copy of his personal information was dated and he felt it necessary to have an updated spreadsheet available for access at work. He attempted to email the encrypted spreadsheet file between his personal and DoD email accounts a couple of times, but the files could not be processed. He said that he then removed the encryption and attached the spreadsheet to emails that he transmitted between his personal and DoD email accounts. (GE 4; AE L)

In April 2020, DoD security personnel notified Applicant that they were conducting a preliminary inquiry into the suspected spillage of classified information attributable to his March 2020 email transmission of a file that included a safe passcode. He confirmed the spreadsheet contained the word "Safe" followed by a passcode for a DoD safe that he previously had access to, and also included his DoD IT network PINs. (AE L at 2-3) He admitted his responsibility for including that information in the spreadsheet. He reported sending approximately four written responses to the DoD security personnel conducting the preliminary inquiry between April 24 and June 2, 2020, "to explain [his] actions and answer questions." (AE L at 3) He has repeatedly claimed that he did not recall the spreadsheet included the DoD Safe passcode when he transmitted the March 2020 emails. He stated that he informed DoD security personnel conducting the preliminary inquiry that he included the DoD information in the spreadsheet "approximately a year ago" or "sometime in early/mid 2019" because that "was the last time [he] had sent the spreadsheet to his [DoD] computer" and because it had been approximately a year since he had access to that safe. (AE L at 3) He also stated that when initially questioned about the incident he admitted that he had made such a transfer "a couple of times in [March] 2020." (GE 4 at 2) He said that he was focused on the suspected March 2020 spillage in his responses, and that he was attempting to only answer the question asked, because he was sensitive to engineers' reputation for being too long-winded in their responses. (GE 4; AE L; Tr. 58-61, 74-76)

Applicant has stated that prior to submitting his June 4, 2020 response, he was anxious that the Government's "concern could now be about my long-term transferring of my file. My mind was fixed, however, on the thought that I needed to answer the question that was being asked (my March 2020 infraction) and that it was not correct to bring in a new 'broader' email concern." (AE-L at 3) He also noted that if he could have discussed details of his compromise with someone other than a direct security manager, it would have been possible for him to discuss his use of the spreadsheet in the context of the Guideline E allegations. (GE 2, 4; AE L; Tr. 35-36, 74-76)

DoD security personnel determined that on about March 5, 2020, Applicant transmitted the spreadsheet including a passcode that identified the combination to a DoD safe, and PIN numbers for access to his DoD sponsor's facility, unclassified and classified DoD IT networks, and his DoD ID card. A preliminary inquiry found that the spreadsheet contained classified information. Further analysis by security personnel determined that he had transmitted a version of the spreadsheet including sensitive DoD information from his unclassified DoD email account to his personal email account approximately once a week (223 times) from at least 2015 to March 2020, and that over a period of several years he appeared to routinely update sensitive DoD information in the spreadsheet, including the safe passcode in 2017. (GE 1, 2, 4; AE L; Tr. 49, 79-99)

In his July 2020 security clearance application (SCA), Applicant reported that he had been warned or disciplined in April 2020, because he "sent FOUO Information (PII) in an unclassified email environment," and "stored and sent classified information within an unclassified email environment." (GE 1 at 12-13) He reported that his security clearance eligibility/access had been suspended in June 2020 because he "sent classified information within an unclassified environment." (GE 1 at 39)

Applicant stated that in June 2020, he learned that the DoD security concerns were his long-term transmission of a spreadsheet, and lack of transparency about his conduct. He said that he "made full disclosure of [his] actions at [his] next opportunity, which was during his [security clearance background interviews]" in July and August 2020. (AE L at 3) During those background interviews with a government investigator, Applicant said that he had transmitted the spreadsheet as an encrypted file between his personal and DoD email accounts. He reported that in March 2020, he unsuccessfully attempted to email the encrypted spreadsheet file between his personal and DoD email accounts a couple of times, "but the files could not be processed." (GE 4 at 1, 2) He said that he then removed the encryption and transmitted the spreadsheet. When asked why he had tried to send the encrypted file after a policy prohibiting that practice was instituted, he said that policy was neither written nor explicit and that when he had previously tried to send an encrypted file and the system would not permit its transmission, he had assumed, or it was implied that transmission of encrypted documents was prohibited by policy. (GE 4 at 5-6) He said he had forgotten the spreadsheet included his classified DoD IT network PIN, DoD ID PIN, and safe passcode. He also told a background investigator that he had added the DoD safe passcode to the spreadsheet approximately a year earlier and sent those files to himself via email. (GE 4 at 3) He said that he last accessed classified documents in the safe in mid-2019, while working for a previous employer. He also said that the safe had since been relocated and was no longer used for classified storage. He acknowledged that he was not supposed to store classified information with personal information, and said that he had been trained on and was aware of policies regulating the use of DoD email, and the protection of sensitive and classified information. (GE 4)

Applicant admitted the allegations at SOR ¶¶ 1.a, 1.b, 2.a, and 2.b, with explanations; admitted, in part, and denied, in part, allegations at SOR ¶¶ 1.c, and 2.c, and denied the allegation at SOR ¶ 2.d. (SOR Response)

SOR ¶¶ 1.a, 1.b, and 2.a allege that in about March 2020 Applicant improperly sent an email with an attachment that contained sensitive DoD information, including network and facility access PINs, and a safe combination, and that an inquiry determined that the spreadsheet sent from his DoD email to his personal email account contained classified information. In response to the SOR, he admitted the allegations at SOR ¶¶ 1.a, 1.b, and 2.a, explaining that he had intended to transmit his personal information, but had forgotten that he had previously included sensitive DoD information in the spreadsheet. He said that he had been told this information was not classified, that he had previously included it in the file because he feared that he might forget the access information, and that his conduct was an inadvertent, isolated event. (SOR Response)

SOR ¶¶ 1.c and 2.c allege that Applicant exhibited a prolonged pattern of behavior that endangered DoD information security, and that between 2015 and 2020 he routinely updated sensitive DoD information in the spreadsheet file he sent between his DoD and personal email accounts including a safe passcode, and that those actions contradicted written statements he provided to security officials. In response to the SOR he admitted, in part, and denied, in part, those allegations explaining that:

> I sent my personal file to my personal email. I would do this periodically to provide myself updates regarding my [personal information]. Approximately a year prior to the security incident, I included the sensitive information in my personal file so I would not forget it in case I needed to lock up something classified. I did this so long ago, that when I sent the file, I had forgotten the sensitive information was also included. . . . The file contained my personal information, which I would occasionally update if necessary. When making my written statements, I stated that "approximately a year ago, I included this information" in reference to the sensitive information included in the file update I sent in March 2020.

(SOR Response at 2, 4)

SOR ¶ 2.b alleges that about once a week from 2015 to March 2020, Applicant emailed a spreadsheet containing his own personal information, including financial, medical, and commercial account access codes, from his work email account to his personal email account. He admitted the allegation noting that the spreadsheet was encrypted, except for transmissions in March 2020. (SOR Response at 3-5).

SOR ¶ 2.d alleges that he was likely aware that he was mishandling sensitive data, that he provided misleading responses to security officials investigating the matter, and that he misled officials about the nature and extent of his behavior. He denied that allegation, stating that he truthfully answered questions from security officials. (SOR Response at 2, 4)

The Government submitted an Information Security Program instruction, effective March 22, 2018, for the DoD agency that Applicant had supported. The instruction states that Controlled Unclassified Information (CUI) applies to Unclassified Information to which

access or distribution limitations may be applied including information eligible for marking as "For Official Use Only" (FOUO). The instruction applies to on-site contractors and prohibits transmission of that agency's CUI to personal electronic accounts, and requires contractor personnel complete Information Security training annually. (GE 5 at 10, 32, 54)

Applicant testified that from at least 2015 to March 2020, he transmitted a spreadsheet that included a passcode for a DoD safe used to store classified information between his DoD and personal email accounts. (Tr. 58-64) He said the word "Safe" was followed by a six letter word that correlated to the safe's numerical combination, but did not specify the safe's location or number. (Tr. 60-64; AE l at 1-3) He testified that he was notified in April 2020 that the presence of safe password in an email attachment was being investigated as spillage of classified information. (Tr. 59-60) He disputed that the spreadsheet included classified information, stating that he understood from training that a piece of information without context was not by itself classified. (Tr. 26-29; AE L at 2). He testified that he believed that his DoD PINs including his classified IT network, facility access, and ID card PINs were sensitive, but not classified information. (Tr. 30-32, 35, 48-51, 64-67; AE L at 2) He acknowledged that he had not asked whether the aforementioned DoD information was classified or not. (Tr. 48) He said that he notified his company's security officer about the potential March 2020 spillage, after he was informed of the suspected spillage by a DoD security officer in April 2020. (Tr. 35-36, 50-52) He testified that he did not disclose that he had updated DoD sensitive information in the spreadsheet for a number of years because he was focused on the unencrypted March 2020 email. (Tr. 34-35) He said that he did not understand the concern was about "the issue over the extended period of time since 2015," until June 2020 after his company received a letter explaining why his facility access had been revoked. (Tr. 51-52, 74-76). He testified that he had complied with post-incident counselling, and had removed all DoD sensitive information from the spreadsheet. (Tr. 35-36)

He testified that he kept back-up copies of the spreadsheet including the sensitive DoD information on his home computer and in a commercial storage system. (Tr. 64). He said that prior to March 2020, the spreadsheet file was encrypted in order to protect the contents. He noted that it was regular practice at the agency he supported, and consistent with his training to encrypt CUI and FOUO information transmitted via unclassified email. (Tr. 28-29) He explained that he had reported transmitting classified information in his SCA, because he was answering the questions that were asked. He testified that he had truthfully answered all investigator and SCA questions, based upon his understanding of those questions at the time. (Tr. 35) He also testified that sometime in 2019 the DoD agency he supported prohibited the transmission of encrypted emails to and from that agency. (Tr. 39-40)

A DoD counter-insider threat security official testified that investigation determined that the spreadsheet included classified and sensitive DoD information. (Tr. 78-99) He said that Applicant's classified network PIN, which could be used in conjunction with a chipped card to gain access to a classified DoD IT network was determined to be classified. (Tr. 94-99) He testified that the PIN for the DoD Agency's door ("that's how it was labeled"), his DoD-issued identification card PIN, and the safe passcode were

sensitive DoD information. (Tr. 86, 96-99) He also testified that there was no evidence that the classified information had been intentionally leaked or otherwise compromised. (Tr. 83, 94)

Applicant provided documentary evidence that he has an excellent reputation, and has established a sound record of performance for his employers and the DoD entities they support. Information provided in this regard notes his reliability, good character, and recognized technical skills. Many of his personal references are familiar with the SOR allegations and expressed no reservations about recommending him for a security clearance. He also received numerous awards and was active in his community. In May 2020, Applicant was counseled on his employer's and sponsoring DoD agency's policies regarding handling sensitive information. (SOR Response; AE A-L)

Policies

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 an 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.

When evaluating an applicant's suitability for national security eligibility, the administrative judge must consider the adjudicative guidelines (AG). In addition to brief introductory explanations for each guideline, the adjudicative guidelines list potentially disqualifying conditions and mitigating conditions, which are used 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 overarching adjudicative goal is a fair, impartial, and common sense 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.

Under Directive ¶ E3.1.14, the Government must present evidence to establish controverted facts alleged in the SOR. Directive ¶ E3.1.15 states an "applicant is responsible for presenting witnesses and other evidence to rebut, explain, extenuate, or mitigate facts admitted by the applicant or proven by Department Counsel, and has the ultimate burden of persuasion as to obtaining a favorable clearance 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." Section 7 of EO 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

AG ¶ 33 articulates the security concern for handling protected information:

> 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.

AG ¶ 34 provides conditions that could raise a security concern and may be disqualifying. The following are potentially applicable:

> (b) collecting or storing protected information in any unauthorized location;
>
> (c) loading, drafting, editing, modifying, storing, transmitting, or otherwise handling protected information, including images, on any unauthorized equipment or medium; and
>
> (g) any failure to comply with rules for the protection of classified or sensitive information.

Applicant admitted that he improperly sent an email with an attached spreadsheet containing sensitive DoD information in March 2020 (SOR ¶ 1.a). He acknowledged that a preliminary inquiry concluded that the spreadsheet he transmitted from his unclassified DoD email account to his personal email account contained classified information and that the transmission of classified information over unclassified networks was prohibited, but has repeatedly stated his belief that the spreadsheet did not contain classified information. (SOR ¶ 1.b). The Government presented substantial, unrebutted evidence that the spreadsheet contained classified information including documentary evidence that it contained unspecified classified information, and testimony that Applicant's classified IT network PIN was classified information. AG ¶ 34(b) and 34(c) apply.

In response to SOR ¶ 1.c, Applicant admitted that he periodically sent a spreadsheet containing his personal information from his DoD email to his personal email account, that he had included CUI in the spreadsheet since about March 2019, and that when he sent the March 2020 email he had forgotten the spreadsheet contained CUI.

The Government presented substantial, unrebutted evidence that Applicant transmitted a spreadsheet containing protected DoD information from his DoD email account to his personal email account approximately 223 times from 2015 to March 2020, and that, since at least March 22, 2018, he was prohibited by regulation from transmitting CUI from his DoD email account to his personal email account. AG ¶¶ 34(b), 34(c), and 34(g) apply.

Conditions that could mitigate handling protected information security concerns are provided under AG ¶ 35. The following 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;
>
> (c) the security violations were due to improper or inadequate training or unclear instructions; and
>
> (d) the violation was inadvertent, it was promptly reported, there is no evidence of compromise, and it does not suggest a pattern.

Security violations "strike at the heart of the industrial security program" and are one of the strongest possible reasons for denying or revoking access to classified information, because they raise serious questions about an applicant's suitability for access to classified information. ISCR Case No. 03-26888 at 1 (App. Bd. Oct. 5, 2006). Once it is shown that an applicant has committed such violations, he or she has a "very heavy burden" in demonstrating mitigation. ISCR Case No. 14-05127 at 8 (App. Bd. June 24, 2016).

AG ¶ 35(a) does not apply. Applicant improperly handled and transmitted protected DoD information frequently and recently (223 times from 2015 to March 2020). He routinely stored, reviewed, revised, and transmitted a spreadsheet containing protected DoD information including classified information between his DoD and personal email accounts for personal convenience. He has provided inconsistent accounts of his actions including how long he maintained protected information in the spreadsheet, whether any of that information was classified, and whether or when he was prohibited from transmitting CUI to his personal email account in an encrypted file or otherwise. He has presented insufficient evidence to support a conclusion that the behavior is unlikely to recur, or that it does not cast doubt on his current reliability, trustworthiness, or good judgment.

AG ¶ 35(b) does not fully apply. Applicant was counselled by his employer on policies regarding the proper handling of sensitive information after the March 2020

incident, and has expressed regret for sending the spreadsheet as an unencrypted file in March 2020. However, he has provided insufficient evidence to demonstrate a positive attitude towards the discharge of security responsibilities.

AG ¶ 35(c) does not apply. Applicant acknowledged that he had been trained on information security and the proper handling of classified and sensitive information including periodic refresher training prior to the March 2020 incident.

AG ¶ 35(d) does not apply. Applicant routinely updated and transmitted the spreadsheet including protected DoD information to and from his personal email account from at least 2015 to March 2020. He first reported his security violation approximately one month after his March 2020 email transmission, after DoD security officials had notified him that his email transmission was being investigated as suspected spillage of classified information.

Handling protected information security concerns are not mitigated.

Personal Conduct

The security concern for personal conduct is set out in AG ¶ 15, as follows:

> Conduct involving questionable judgment, lack of candor, dishonesty, or unwillingness to comply with rules and regulations can raise questions about an individual's reliability, trustworthiness, and ability to protect classified or sensitive information. Of special interest is any failure to cooperate or provide truthful and candid answers during national security investigative or adjudicative processes. The following will normally result in an unfavorable national security eligibility determination, security clearance action, or cancellation of further processing for national security eligibility:

AG ¶ 16 lists conditions that could raise a security concern and may be disqualifying in this case including:

> (b) deliberately providing false or misleading information; or concealing or omitting information, concerning relevant facts to an employer, investigator, security official, competent medical or mental health professional involved in making a recommendation relevant to a national security eligibility determination, or other official government representative;
>
> (d) credible adverse information that is not explicitly covered under any other guideline and may not be sufficient by itself for an adverse determination, but which, when combined with all available information, supports a whole-person assessment of questionable judgment, untrustworthiness, unreliability, lack of candor, unwillingness to comply with rules and regulations, or other characteristics indicating that the individual

may not properly safeguard classified or sensitive information. This includes, but is not limited to, consideration of:

> (1) untrustworthy or unreliable behavior to include breach of client confidentiality, release of proprietary information, unauthorized release of sensitive corporate or government protected information;
>
> (2) any disruptive, violent, or other inappropriate behavior;
>
> (3) a pattern of dishonesty or rule violations; and
>
> (4) evidence of significant misuse of Government or other employer's time or resources; and

(e) personal conduct, or concealment of information about one's conduct, that creates a vulnerability to exploitation, manipulation, or duress by a foreign intelligence entity or other individual or group. Such conduct includes:

> (1) engaging in activities which, if known, could affect the person's personal, professional, or community standing[.]

SOR ¶ 2.a cross-alleges the conduct alleged in SOR ¶¶ 1.a and 1.b and is equally a security concern under the personal conduct guideline. Applicant's transmission of a spreadsheet containing protected DoD information including classified information to his personal email account damaged his personal, professional, and community standing, and created vulnerability to exploitation, manipulation, or duress. AG ¶ 16(e) is established.

SOR ¶ 2.b alleges under the personal conduct guideline that about once a week, from 2015 to March 2020, he emailed a version of the spreadsheet containing his own personal data from his DoD email to his personal email account. Applicant repeatedly stated that he encrypted the spreadsheet in every email transmission except in March 2020. No evidence from a witness, a regulation, an investigation, or similar source was presented to contradict his statements. There is insufficient evidence to support a conclusion that Applicant's transmission of his own personal information via encrypted email raised a security concern under Guideline E. To the extent that any personal conduct security concern may have been raised by his unencrypted transmission of his own personal information in March 2022, that concern is mitigated, because the behavior was infrequent, he has since acknowledged and been counselled on that behavior, that behavior is unlikely to recur and does not cast doubt on his current reliability, trustworthiness, or good judgment. I find for Applicant on the allegation in SOR ¶ 2.b.

With respect to SOR ¶¶ 2.c and 2.d, the record as whole reflects that from at least 2015 to March 2020 Applicant maintained and updated protected DoD information in a spreadsheet that he routinely transmitted between his DoD email and personal email

accounts, and that those actions contradicted written statements he provided to DoD security officials inquiring into the suspected spillage of classified information contained in the spreadsheet attached to his March 2020 email. For AG ¶ 16(b) to apply to the conduct alleged in SOR ¶¶ 2.c and 2.d, Applicant had to deliberately provide false or misleading information or deliberately omit information relevant to security officials.

Applicant has admitted that in written statements to DoD security officials conducting a preliminary inquiry into the suspected compromise of classified information that he stated that he included sensitive DoD information in the spreadsheet for approximately one year prior to March 2020. He subsequently admitted that he included the Safe passcode and other sensitive information in the spreadsheet from at least 2015 to March 2020, and that he had routinely emailed that information between his DoD and personal email accounts during that timeframe. Applicant denies that he deliberately misled those security officials. When an allegation of falsification is controverted, the Government has the burden of proving it. Proof of an omission, standing alone, does not establish or prove an applicant's intent or state of mind when the omission occurred. An administrative judge must consider the record evidence as a whole to determine an applicant's state of mind at the time of a falsification or omission. *See* ISCR Case No. 03-09483 at 4 (App. Bd. Nov. 17, 2004) (citation omitted).

Considering the record as a whole, I do not find Applicant's claims that he did not intentionally mislead the DoD personnel conducting the preliminary inquiry credible. His written response that he had included the sensitive DoD information in the spreadsheet approximately a year before March 2020 was false or, at a minimum, incomplete. I conclude that he either deliberately falsified this information, or deliberately omitted information key to determining the duration of his conduct for the following reasons.

First, his explanation that he made the statement because that was the last time that he had sent the spreadsheet to his DoD computer is contradicted by evidence that he transmitted the spreadsheet approximately weekly from 2015 to March 2020. Second, I find his claim that he made that statement because that was the last time he had accessed the DoD safe unpersuasive in the context of a preliminary inquiry into the suspected spillage of classified information in an unclassified email. Third, he repeated the claim that he had added the safe passcode to the spreadsheet approximately a year prior to the March 2020 incident to a background investigator in July 2020. This is notable because he claimed that he fully disclosed the scope of his conduct in that background interview after learning that DoD was concerned about his long-term transmission of the spreadsheet. Finally, Applicant's insight into his own state of mind at the time supports a conclusion that he deliberately omitted information about the duration of his conduct. Specifically, he acknowledged that he considered disclosing his long-term transmission of the protected DoD information to officials conducting the preliminary inquiry, but did not do so, because in the context of the question asked and based upon his own mindset, he decided "that it was not correct to bring in a new 'broader' email concern." (AE-L at 3).

Based on all the evidence, I find that the Government has established that the Applicant deliberately provided false information, or intentionally omitted information

about how long he maintained protected information in the spreadsheet to DoD security officials conducting the preliminary inquiry. AG ¶ 16(b) applies. When the same conduct is alleged twice in the SOR under the same guideline, as in SOR ¶¶ 2.c and 2.d, one of the duplicative allegations should be resolved in Applicant's favor. *See* ISCR Case No. 03-04704 at 3 (App. Bd. Sep. 21, 2005). Therefore, SOR ¶ 2.d is concluded for Applicant.

Three mitigating conditions under AG ¶ 17 are potentially applicable in this case:

> (a) the individual made prompt, good-faith efforts to correct the omission, concealment, or falsification before being confronted with the facts;
>
> (c) the offense is so minor, or so much time has passed, or the behavior is so infrequent, or it happened under such unique circumstances that it is unlikely to recur and does not cast doubt on the individual's reliability, trustworthiness, or good judgment; and
>
> (d) the individual has acknowledged the behavior and obtained counseling to change the behavior or taken other positive steps to alleviate the stressors, circumstances, or factors that contributed to untrustworthy, unreliable, or other inappropriate behavior, and such behavior is unlikely to recur.

AG ¶I¶ 17(a), 17(c), and 17(d) do not apply. Applicant's conduct was serious and frequent. He routinely updated protected DoD information in a spreadsheet that he maintained outside of a DoD network, and, from 2015 to March 2020, transmitted that protected information at least 223 times between his unclassified DoD and personal email accounts. In March 2020, he transmitted an email with sensitive and classified DoD information from his DoD to his personal email account that created a vulnerability to exploitation or manipulation. When questioned by DoD security officials inquiring into the suspected spillage of classified information contained in his March 2020 email, he deliberately misled those officials about the duration of his conduct. Although he acknowledged the behavior and was counseled by his employer, there is insufficient evidence to support a conclusion that the behavior is unlikely to recur, or that Applicant made prompt good-faith efforts to correct his omission or falsification before being confronted with the facts.

Based upon the entire record, I cannot find that such behavior is unlikely to recur and do find that his conduct continues to cast doubt on his reliability, trustworthiness, and good judgment. Guideline E security concerns are not mitigated.

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(d):

> (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 considered the potentially disqualifying and mitigating conditions in light of all the facts and circumstances surrounding this case. I have incorporated my comments under Guideline K, and Guideline E in my whole-person analysis. Some of the factors in AG ¶ 2(d) were addressed under those guidelines, but some warrant additional comment.

I considered that Applicant is 56-years-old, held an active security clearance from 1988 to at least June 2020, and received regular training on information security and the proper handling of classified information. I considered that he has worked on significant defense projects since 1990, has an excellent reputation for reliability, good character, recognized technical skills, and has a sound record of performance. I also considered that there is no evidence that the protected information contained in the spreadsheet was compromised and that he was counselled on the proper handling of sensitive information after the March 2020 incident.

However, when faced with the common modern day challenge of keeping track of DoD passwords and PIN codes necessary to perform his duties, Applicant exercised poor judgment and decided to integrate that information into a spreadsheet that included extensive personal information. From at least 2015 until March 2020 he stored the spreadsheet on private servers, updated, and routinely transmitted it between his unclassified DoD and personal email accounts. Although the DoD agency he supported had prohibited the transmission of CUI to personal electronic accounts since at least March 2018, and notwithstanding his understanding that agency had prohibited the transmission of encrypted emails outside of DoD sometime in 2019, he transmitted encrypted versions of the spreadsheet in 2019, and attempted to do so again in March 2020. When he could not successfully transmit the encrypted spreadsheet file, he removed the encryption and transmitted it between his personal and DoD email accounts because he wanted to have access to his personal information at work.

Applicant apparently believed that he had diluted the details of the DoD information to such a degree that he could permissibly maintain and transmit that information outside of DoD systems, but DoD security officials disagreed. Those officials determined that the spreadsheet contained both sensitive and classified DoD information. When questioned about his suspected spillage of classified information, Applicant deliberately misled DoD

officials about how long he had maintained that information, and understated how many times he had transmitted it. In an SCA completed in June 2020, he disclosed that he had been disciplined and that his security clearance access had been suspended because he had sent FOUO Information, and stored and sent classified information in an unclassified email environment. He has since disputed, without corroborating evidence, that the spreadsheet contained classified information.

After weighing the disqualifying and mitigating conditions under Guidelines K and E, and evaluating all the evidence in the context of the whole person, I conclude Applicant has not mitigated the security concerns based on handling protected information or personal conduct. Accordingly, I conclude he has not carried his burden of showing that it is clearly consistent with the national interest to continue his eligibility for access to classified information.

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.c:	Against Applicant
Paragraph 2, Guideline E:	AGAINST APPLICANT
Subparagraphs 2.a and 2.c:	Against Applicant
Subparagraphs 2.b and 2.d:	For Applicant

Conclusion

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

_____
Eric C. Price
Administrative Judge