DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 19-03928
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Andrew Henderson, Esq., Department Counsel
For Applicant: Ryan C. Nerney, Esq.

March 25, 2022

_____

Decision

_____

TUIDER, Robert, Administrative Judge:

Applicant mitigated security concerns under Guidelines M (use of information technology) and K (handling protected information). Eligibility for access to classified information is granted.

Statement of the Case

On February 3, 2018, Applicant submitted a Questionnaire for National Security Positions (SF-86). On February 2, 2021, the Defense Counterintelligence and Security Agency Consolidated Adjudications Facility (CAF) issued a Statement of Reasons (SOR) to Applicant detailing security concerns under Guidelines M and K. The SOR detailed reasons why the CAF was unable to find that it is clearly consistent with the national interest to grant or continue a security clearance for Applicant.

On February 17, 2021, Applicant submitted his Answer to the SOR through former counsel, and elected to have his case decided on the written record in lieu of a hearing. However, on March 29, 2021, Department Counsel, pursuant to Paragraph E.3.1.7 of the Additional Procedural Guidance at Enclosure (3) of DOD Directive

5220.6, requested a hearing in subject case. Accordingly, the case was converted from an administrative decision to a hearing. On March 29, 2021, Department Counsel was ready to proceed.

On April 8, 2021, the Defense Office of Hearings and Appeals (DOHA) assigned the case to me. On April 8, 2021, DOHA issued a notice scheduling the hearing for May 17, 2021. The hearing was convened as scheduled. Department Counsel offered Government Exhibits (GE) 1 through 4, which I admitted without objection. Applicant testified, did not call any witnesses, and offered Applicant Exhibits (AE) A through O, which I admitted without objection. On May 25, 2021, DOHA received the hearing transcript (Tr.).

Findings of Fact

Background Information

Applicant is a 41-year-old director of engineering employed by a defense contractor since July 2003. He was granted a secret security clearance "a couple of years" after he began his employment. Although he does not require a clearance to maintain his current position, he seeks to reinstate his clearance to enhance his position within his company. (Tr. 10-12, 15; GE 1)

Applicant graduated from high school in May 1999. He was awarded a bachelor of science degree in electrical engineering with a 3.95 GPA and received the Bronze Tablet award for graduating in the top 1% of his class in May 2003. He was awarded a master's degree in electrical engineering with a 3.93 GPA in May 2005, graduating in the top one percent of his class. (SOR Answer; Tr. 12-14, 52; GE 1; AE C, AE I, AE J) Applicant married in November 2008. He and his wife have two minor children. (Tr. 14-15; GE 1)

Use of Information Technology/Handling Protected Information

The concerns identified under these Guidelines are listed as four separate allegations and are discussed below in order as listed in the SOR.

SOR ¶ 1.a – Alleged that Applicant created an unclassified presentation that contained classified information, accessed the presentation on two or more company computers, and when questioned by his company security office, he only informed them of one computer.

Applicant admitted this allegation with explanation. In June 2016, Applicant created and saved "with some assistance from other colleagues" an unclassified presentation on a company unclassified shared drive. He took "great care to ensure that the entire presentation was unclassified." (SOR Answer; Tr. 17, 42-43) Multiple company employees used Applicant's presentation and saved it in an unclassified network drive. One of those employees thought there was some classified information on the presentation. (SOR Answer; Tr. 17-18)

Applicant accessed the presentation on three different company computers by navigating to the link on the network drive and opening that link. The presentation was stored on the network drive. (Tr. 18) When questioned by the security office, Applicant was asked where he stored the presentation and he informed them that he stored it on the network drive. The presentation was not stored on more than one computer. However, any computer connected to the network drive could access it. (Tr. 18-19) Applicant stated that the presentation did not contain any classified information. Applicant knows that to be true because he reviewed the information with the security office, along with the Security Classification Guide for the program. Applicant and the security office agreed that the information in question was not classified. (Tr. 19-20)

Applicant did not actually download or save the presentation onto any computer. Rather, he had created the presentation on his own computer and saved it only on an unclassified shared drive. (SOR Answer) When asked by the security office whether the presentation was on any other computers, Applicant perceived this question to relate to only the downloading and saving of the presentation to a computer, not the mere accessing of the presentation on the shared drive via a computer. Therefore, he answered in the negative, even though he had accessed the presentation on the shared drive via a total of three computers. Applicant stated this was an honest misunderstanding and interpreted the security office's inquiry in the literal sense. (SOR Answer)

Applicant stated that he never attempted to conceal the fact that he had accessed the presentation on three separate computers. He advised the security office that the presentation was saved to an unclassified shared drive, and therefore would have been accessible by multiple users from any network-connected drive. Applicant was well aware that the company's computer security officials could easily and immediately determine all users and/or devices that had accessed the presentation after it was saved to the unclassified shared drive. (SOR Answer)

The security office and Applicant noted that the questioned material had been publicly released and was readily accessible through open sources in the public domain. Applicant received no follow-up from the security office on this matter. His computer was returned to him. He was not cited for a security infraction. Applicant's presentation still remains on the company unclassified shared drive, where he originally saved it. (SOR Answer; Tr. 53-55)

Applicant accessed this presentation on more than one company computer because the presentation was stored on a server. Sometimes, he would not be at his normal workstation and when he found himself at different locations, he would pull the presentation from the server and review it. (Tr. 22) As a take away from this incident, Applicant has vowed to read the Security Classification Guide as the first order of business before working on a particular new program. In a typical year, Applicant creates "[t]housands probably" of presentations. (Tr. 20-21)

SOR ¶ 1.b – Alleged that Applicant used a colleague's account to access a DoD classified system after his account had lapsed.

Applicant admitted this allegation with explanation. On infrequent occasions, Applicant visited the company lab without having first obtaining a current group password (i.e. the former group password has expired and Applicant had not yet gone through the administrative process to obtain the new one). Applicant was unsure of the exact date when this occurred, and on cross-examination settled on the approximate date of 2013. On these infrequent occasions, a company colleague would log in to the group account on Applicant's behalf. (SOR Answer; Tr. 22-23, 25, 42-43)

The lab environment involved multiple cleared individuals who typically shared a computer or computers in a secure place. The practice of one person logging on with the current group password and others doing the same was relatively common and an accepted practice of his coworkers. The Director of Integration and Testing, a company colleague of Applicant, provided the following about the group account access practices in the lab:

> I worked with [Applicant] on the [program] from 2008-2017. [Applicant] had the clearance and the need to know to view classified data associated with the system. The program has many different computer accounts and systems. Many of the computer labs had shared computers. Employees were responsible for ensuring they kept the accounts up to date and remembering the latest group account password. Our satellite integration and test occurred at an offsite customer facility. For people in managerial roles and travelers to our site, like [Applicant], that only used these systems occasionally; it was not unusual to have their account or password not be up to date. In these labs with shared computers, it was not unusual for one person to login on a group account or their account and have another person access or view test data (while the user was in the room). This was considered acceptable as long as the person was cleared, had need to know and was authorized to view the data. (SOR Answer (Tab D))

Applicant reiterated what Director of Integration and testing stated above during his testimony. (Tr. 23-24) Applicant understands that password sharing of the sort mentioned above is not permitted and inappropriate, even in a group password and group account environment. He pledged to obtain and use a current group password on visits to the company lab on all future occasions. He understands clearly that he must personally obtain a current group password, and that it is improper for a colleague to log into a group account on his behalf. Of note, there was an identical group password for all users of the group account. At all times in question, Applicant was eligible to obtain the group password renewals. He held the proper clearance to access the group account, and always had the need to know. (SOR Answer; Tr. 25-26)

SOR ¶ 1.c – Alleged that Applicant used classified material that was removed without approval, and saved the product in two locations on an unclassified company server. He did not report this incident to company security.

Applicant denied this allegation with explanation. He explained that a cleared colleague (CC) strictly followed all protocol and procedures for the transfer of unclassified data from a classified system (high side) to an unclassified system (low side). He properly exported the data from the high side to the low side, where he saved it. (SOR Answer; Tr. 26-27) Applicant was unsure of the timeframe when this occurred, stating it was "around 2013 maybe. But since it's been so long, I don't remember the exact year. It was before 2015." (Tr. 30, 44)

After the data had been exported to the low side, Applicant included a portion of it in two presentations he created and saved on an unclassified company computer. When CC reviewed Applicant's presentation, he recommended that Applicant delete a small portion of it. CC knew the entire presentation was unclassified, but he believed the audience seeing the presentation might erroneously believe that the small portion was classified, and he did not want to take presentation time to explain why the material was unclassified. Applicant deleted the small portion of the presentation, per CC's suggestion. (SOR Answer; Tr. 27-29) CC states as follows:

> I worked with [Applicant] in the support of a program in which we analyzed performance data of an electronics unit in the 2014 to 2016 time frame that was saved on a classified system. The performance data was unclassified. OPSEC CONOPs was followed correctly to remove the unclassified data from the system. We were allowed to print unclassified plots, stamp them "UNCLASS" and take them outside the classified labs. The data was unclassified when removed from the lab. Out of abundance of caution, additional security guidelines were taken into account as we prepared the plots of the data for presentation. The data was already unclassified, but this additional step made it more obvious the data was unclassified, allowing the presentation to be made without having to explain why the data was unclassified. (SOR Answer (Tab D))

As the above evidence indicates, no security violation occurred that required making a report to company security. Applicant stated that even though he did not compromise any classified information and did not violate any policies, there is always more one can do when it comes to security and protecting classified information. It is better to be even more "hyper-vigilant" and take every possible precaution when it comes to protecting classified information. (Tr. 29-39)

SOR ¶ 1.d – Alleged that between about 2009 to at least 2016 Applicant accessed a Government computer system without authorization once or twice a year. He had "viewing privileges" only so he circumvented this by downloading test data to a computer he was not authorized to access and then having a colleague transfer data to his computer. (Tr. 44-45)

Applicant denied this allegation with explanation. He explained the situation described in the SOR is not an altogether accurate depiction of the facts. Similar to the situation described in SOR ¶ 1.b, above., Applicant held the proper clearance to access the classified systems in question. He was also eligible to obtain an updated group

password. However, he had not gone through the administrative process to obtain the most recent group password for the group accounts involved. In this instance, Applicant was visiting a company site in another city, and the person responsible for providing updated passwords was absent from the office on the day in question. (SOR Answer; Tr. 30-31)

The testing data involved in this situation was unclassified. Applicant needed to perform data analysis on the relevant unclassified testing data. The unclassified testing data resided on the "first classified system," but this system did not offer the analytical tools Applicant needed to properly process the data. A "second classified system" offered these tools. (SOR Answer) Applicant asked his colleague to transfer the relevant unclassified testing data from the "first classified system" (the one without the analytical tools he needed) to the "second classified system" (the one with the analytical tools he needed). This transfer did not require Applicant to access the "first classified system," and he did not do so. Once the unclassified testing data was transferred to the "second classified system," Applicant performed analysis using the tools offered by "second classified system." (SOR Answer; Tr. 31)

Applicant was properly cleared to access both the "first classified system" and the "second classified system." However, he had not administratively obtained an updated group password for either system. His colleague logged on to the "second classified system" on his behalf, so that Applicant could access and analyze the unclassified testing data that had been transferred from the "first classified system." (SOR Answer; Tr. 32) The allegation that Applicant accessed a Government computer system without authorization once or twice a year is not true, because Applicant was cleared and had a need to know that information. (Tr. 32)

The "second classified system" was not Applicant's computer, as stated in the SOR. The two "systems" were not computers, but rather they were group accounts on classified systems accessible via a current group password. (SOR Answer) Applicant performed analysis of the unclassified testing data on the "second classified system." He did not remove any of the unclassified testing data from the "second classified system" when he did so. (SOR Answer; Tr. 32-34) Applicant has not had a similar situation occur like this "since 2016." (Tr. 33) Applicant learned as a take away from this event that everyone allowed into the facility would be required to know the group username and password as an additional safeguard to protect classified information. (Tr. 34-35)

Applicant reiterated throughout his testimony that these incidents have instilled in him a heightened sense of security awareness. (Tr. 20-22, 29, 34-35) Applicant has since taken numerous security training courses, and submitted seven certificates of completion for various security training courses. (Tr. 21, 35-36, 38; AE O)

The Government cross-alleged the use of information technology concern raised in SOR ¶¶ 1.a through 1.d as an additional handling protected information allegation under SOR ¶ 2.a. The facts and mitigation discussed under use of information technology are applicable to the handling protected information concern.

To summarize and clarify, the last time Applicant engaged in any type of "similar incidents was "about 2016," approximately five years before his hearing date. (Tr. 36) Applicant stated that he never engaged in behavior that resulted in the compromise of classified material. (Tr. 36) Applicant's company never found that he failed to properly follow its policies, regulations, procedures, or mishandled classified material. (Tr. 36) Nor did his company find that Applicant misused any information technology. (Tr. 37) Furthermore, Applicant's company never determined that he lied or lacked candor when explaining or discussing these events with them. (Tr. 37) None of these SOR allegations led to Applicant being disciplined by his company. (Tr. 37)

Applicant has since taken a behavior modification course following these incidents to avoid making similar mistakes in the future. He learned how one's personality can effect one's behavior. He realized that his persona is very "task oriented" and "goal oriented," which resulted in him being more focused on getting the job done. He recognizes that he must remain "more hyper-vigilant" when it comes to using security precautions and avoid lapses such as not taking the proper care to know his password. (Tr. 37-38) Applicant submitted a Certificate of Completion dated April 18, 2021, to document his having completed a four-hour behavior modification class and passing a written knowledge assessment. (AE N)

Non-Alleged Conduct

Applicant was denied clearances in 2004, 2006, 2008, and 2018. In 2009, Applicant was granted a clearance. His most recent SF-86 was dated February 3, 2018, and was his ten-year renewal application for that 2009 clearance. However, while holding that clearance, at the request of his employer, Applicant applied for eligibility to access sensitive compartmented information (SCI). This SCI access was on a restricted customer project in Another Government Agency (AGA). The AGA denied Applicant's access to SCI, and on April 2, 2018, notified him by letter identifying the reasons for their denial. (Tr. 45-49, 52; GE 1, GE 3, GE 4)

Applicant's 2004, 2006, and 2008 denials appear to have been based primarily on minimizing his high school illegal drug use. (Tr. 39-40) As noted, the CAF granted Applicant's clearance in 2009. Presumably, his 2004, 2006, and 2008 clearance denials were reviewed when the CAF granted his 2009 clearance.

Applicant's 2018 access to SCI AGA denial addressed issues involving personal conduct. He completed a January 17, 2019 statement to the Office of Personnel Management (OPM) that discussed the personal conduct issues after submitting his February 3, 2018 SF-86. (Tr. 45-48; GE 3, GE 4)

During cross-examination, Department Counsel queried Applicant regarding those personal conduct issues. Applicant provided an answer that mirrored the information he provided in his January 17, 2019 OPM statement, and Department Counsel moved to amend the SOR adding a Guideline E (personal conduct) concern. I denied Department Counsel motion to amend. *See* Transcript for further details and Analysis section below. (Tr. 49-51, 55-56)

Character Evidence

A summary of Applicant's closing comments follows. He recognizes the value of information security and is very grateful to have his current job and career. He takes great satisfaction in having spent the last 18 years of his professional life contributing to the security of the United States. He takes information security very seriously and realizes that he could have done better. With the benefit of hindsight and training, he realizes the importance of adhering to security regulations rather than relying on good intentions. He committed to take whatever additional steps are required to avoid any compromise of classified material if granted a clearance. (Tr. 40-41)

Applicant submitted four character letters, all from company employees who have known him for lengthy periods of time. They attested to his good character and trustworthiness and had first-hand knowledge of the SOR allegations. They support reinstatement of his clearance. (SOR Answer; AE D) Applicant's most recent performance review form the calendar year 2019 ranks him as a "Top Performer," and documents significant contributions to his company and the national defense. (SOR Answer; AE E, AE K) He submitted 11 Certificates of Achievement in recognition of professional accomplishments over the past several years. His numerous awards from his company recognized him for contributing to programs advancing national security, technology, and civil needs. (SOR Answer; AE F, AE J, AE L) Applicant is active in his community, coaching his children's sporting events and volunteering for civic events sponsored by his city of residence. (AE M)

Law and Policies

This case is adjudicated under Executive Order (EO) 10865, *Safeguarding Classified Information within Industry* (February 20, 1960), as amended; DOD Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (January 2, 1992), as amended (Directive); and the adjudicative guidelines (AG), which became effective on June 8, 2017.

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 to be 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, administrative judges apply the guidelines in conjunction with the factors listed in AG ¶ 2, describing the adjudicative process. The administrative judge's overarching 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 national security eligibility will be resolved in favor of the national security."

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 the applicant or proven by Department Counsel." The applicant has the ultimate burden of persuasion to obtain a favorable clearance 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 the applicant may deliberately or inadvertently fail to safeguard classified information. Such decisions entail a certain degree of legally permissible extrapolation of potential, rather than actual, risk of compromise of classified information.

Section 7 of EO 10865 provides that adverse 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 M, Use of Information Technology

AG ¶ 39 describes the security concern about use of information technology:

> Failure to comply with rules, procedures, guidelines, or regulations pertaining to information technology systems may raise security concerns about an individual's reliability and trustworthiness, calling into question

the willingness or ability to properly protect sensitive systems, networks, and information. Information Technology includes any computer-based, mobile, or wireless device used to create, store, access, process, manipulate, protect, or move information. This includes any component, whether integrated into a larger system or not, such as hardware, software, or firmware, used to enable or facilitate these operations.

AG ¶ 40 provides several conditions that could raise a security concern and may be disqualifying:

(a) unauthorized entry into any information technology system;

(b) unauthorized modification, destruction, or manipulation of, or denial of access to, an information technology system or any data in such a system;

(c) use of any information technology system to gain unauthorized access to another system or to a compartmented area within the same system;

(d) downloading, storing, or transmitting classified, sensitive, proprietary, or other protected information on or to any unauthorized information technology system;

(e) unauthorized use of any information technology system;

(f) introduction, removal, or duplication of hardware, firmware, software, or media to or from any information technology system when prohibited by rules, procedures, guidelines, or regulations or when otherwise not authorized;

(g) negligence or lax security practices in handling information technology that persists despite counseling by management; and

(h) any misuse of information technology, whether deliberate or negligent, that results in damage to the national security.

The evidence of record raises AG ¶¶ 40(a), 40(c), 40(d), 40(e), and 40(f). Consideration of mitigating conditions is required.

AG ¶ 41 lists several conditions that could mitigate security concerns:

(a) so much time has elapsed since the behavior happened, or it happened under such unusual circumstances, that it is unlikely to recur and does not cast doubt on the individual's reliability, trustworthiness, or good judgment;

(b) the misuse was minor and done solely in the interest of organizational efficiency and effectiveness;

(c) the conduct was unintentional or inadvertent and was followed by a prompt, good-faith effort to correct the situation and by notification to appropriate personnel; and

(d) the misuse was due to improper or inadequate training or unclear instructions.

Mitigation Applicable to SOR ¶ 1.a. AG ¶ 41(a) is applicable. Applicant created the presentation over five years ago. Someone who viewed the presentation thought it contained classified information. However, a review by the company security office determined that the presentation was unclassified. Furthermore, Applicant did not intentionally conceal the fact that he had accessed the presentation via a total of three computers. A security official asked him whether the presentation was on any other computers. Given the fact that Applicant had not downloaded and saved the presentation to any of the three computers, he honestly thought his negative response was an accurate one. However, the computers could have saved the presentations on all computers where it was viewed through automatic saving processes.

Mitigation Applicable to SOR ¶ 1.b. AG ¶ 41(a) is applicable. Applicant was properly cleared for the group account, and to possess a group password. In this situation, the previous group password had expired and Applicant had not yet gone through the administrative process to obtain the new group password. Additionally, the lab environment involved multiple cleared individuals who typically shared a computer or computers in a secure space. The practice of one person logging on with the group password, and others piggy-backing onto the log-on, was a relatively common one. This practice has since stopped. Applicant understands clearly that he must personally obtain a new group password on all occasions going forward, rather than having a colleague log into a group account on his behalf. In some classified environments, someone with a password will access a computer system, and allow someone with authorization of the appropriate classification level to use the computer system without knowing the password. This process limits the access to the system when the password holder is not present. (This is used in the SCIF at military commissions.)

AG ¶ 41(b) is partially applicable. Applicant visited the lab infrequently, and held the proper security clearance to access the group account. He also had an official purpose for accessing the account. He was eligible to obtain the group password, which was identical for everyone who possessed it.

AG ¶ 41(d) is applicable. Given the Director of Integration and Testing's statement that "it was not unusual for one person to login on a group account or their account and have another person access or view the data," it is clear that the company's instruction and training was lacking, unless there is a separate log-in procedure where users with access, and the time of access are preserved. In this regard, the company has apparently since modified its InfoSec training, to make it clear

that “piggy-backing” on, the password of another, even in a situation involving a group account and an identical group password, is not permitted.

Since this issue came to light, Applicant has been very careful about his access to any group account, and about the importance of personally maintaining his own current passwords. He has since completed numerous security training courses. Applicant demonstrated a positive attitude towards maintaining proper security practices.

Mitigation Applicable to SOR ¶ 1.c. AG ¶ 41(a) is applicable. Cleared colleague (CC) correctly exported the unclassified data from the high-side to the low-side. Applicant included a portion of the data in his presentations. CC did not suggest that Applicant remove the questioned data from the presentations because he believed it was classified. Rather, he did so because he thought that someone in the audience might erroneously believe the data was classified, and he did not want to use presentation time explaining why the data was unclassified. No violation occurred here.

Mitigation Applicable to SOR ¶ 1.d. AG ¶ 41(a) is applicable. Applicant held the proper clearance to access both classified systems, and he was eligible to obtain an updated group password. The previous group password had expired, and Applicant was unable to obtain an updated group password in time for his visit to the company site, as the company employee responsible for supplying updated group passwords was absent on the day in question.

Similar to the situation with the lab, described above, the practice of one person logging on with the group password, and others piggy-backing onto that log on, was a common one at that site. This practice has since stopped. Applicant understands clearly that he must personally obtain the current group password for any systems he accesses, rather than having a colleague login to a group account on his behalf.

AG ¶ 41(b) is applicable. Applicant was visiting a remote company site, and held the proper clearance for accessing the relevant materials in both systems. He had an official purpose for accessing the unclassified testing data, and he was eligible to obtain the updated group password which was identical for everyone who possessed it. No violation with respect to Applicant’s accessing of the classified testing data occurred. The data was unclassified and was properly transferred from one system to another. Moreover, Applicant was authorized to access and analyze the data.

AG ¶ 41(d) is applicable. The evidence suggests that the company’s instruction and training on this point needed to be improved. Applicant advised that the company has modified its corporate OPSEC training, to make it clear that the “piggy-backing” on the password of another, even in a situation involving a group account and an identical group password, is inappropriate and not permitted. Since this issue came to light, Applicant has been exceedingly careful about accessing any group account, and about maintaining current group passwords. As noted, he recently completed security, CI, and InfoSec training, and he maintains a positive attitude toward all security responsibilities and requirements.

Applicant apologized for any lapses in exercising the appropriate level of security awareness described above and gave assurances nothing like this will happen in the future. The last incident of any such lapse occurred in approximately 2016, more than five years before his hearing.

Guideline K, Handling Protected Information

AG ¶ 33 described the security concern about 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 several conditions that could raise a security concern and may be disqualifying:

> (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;
>
> (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;
>
> (d) inappropriate efforts to obtain or view protected information outside one's need to know;
>
> (e) copying or modifying protected information in an unauthorized manner designed to conceal or remove classification or other document control markings;
>
> (f) viewing or downloading information from a secure system when the information is beyond the individual's need-to-know;
>
> (g) any failure to comply with rules for the protection of classified or sensitive information;
>
> (h) negligence or lax security practices that persist despite counseling by management; and

(i) failure to comply with rules or regulations that results in damage to the national security, regardless of whether it was deliberate or negligent.

The potential disqualifying conditions under this concern raised by the record evidence are AG ¶¶ 34(c) and 34(g). Consideration of mitigating conditions is required.

AG ¶ 35 41 lists several conditions that could mitigate security concerns:

(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.

Applicant's SOR responses under this concern are identical and applicable to those under Use of Information Technology. The discussion and analysis under Use of Information Technology, above, is applicable under this section. Hence, the analysis under this section will be limited to identifying applicable mitigating conditions under this guideline for each of the SOR ¶ 2.a cross-allegations from SOR ¶¶ 1.a through 1.d.

Mitigating conditions AG ¶¶ 35(a) and 35(d) are applicable to SOR ¶ 1.a. Mitigating conditions AG ¶¶ 35(a), 35(b), 35(c), and 35(d) are applicable to SOR ¶ 1.b. Mitigating conditions AG ¶¶ 35(a) and 35(d) are applicable to SOR ¶ 1.c. Mitigating conditions AG ¶¶ 35(b), 35(c), and 35(d) are applicable to SOR ¶ 1.d.

Whole-Person Concept

Under the whole-person concept, the administrative judge must evaluate an applicant's national security eligibility by considering the totality of the applicant's conduct and all relevant 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.

The ultimate determination whether to grant national security eligibility must be an overall commonsense judgment based upon careful consideration of the guidelines and the whole-person concept. AG ¶ 2(c). The discussion under Guidelines M and K are incorporated in this whole-person section. However, further comments are warranted.

Applicant is a 41-year-old director of engineering employed by a defense contractor since July 2003. He has a distinguished academic record and professional career. He is a highly valued employee and is the recipient of numerous awards. In that regard, his company had enough confidence in him to promote him to director of engineering where he supervises over 100 employees. Applicant was granted a clearance shortly after he was hired in 2003 and later in 2009. During the past 18 years plus as a defense contractor and apart from past clearance issues, Applicant has been an exemplary employee. Applicant's employer and colleagues fully support him.

Admittedly, Applicant has had some unfavorable clearance history. However, in 2009, he was granted a clearance and while he held that clearance, he applied for SCI access to work on a project for an AGA customer. That access was denied in 2018. The basis of that AGA denial led to the current SOR allegations, which as discussed above, Applicant successfully mitigated.

As noted, Department Counsel moved to amend the SOR to add a personal conduction allegation, a motion I denied. That personal conduct is described in Applicant's January 17, 2019 OPM statement (GE 2), but was not alleged in his February 2, 2021 SOR. The Government was aware of potential personal conduct issues and chose not to allege them in the SOR or at any time up to his May 17, 2021 hearing. I denied the motion to amend primarily out of fundamental fairness concerns, that is, Applicant did not have sufficient notice to enable him to fully address the allegation. In ISCR Case No. 03-20327 at 4 (App. Bd. Oct. 26, 2006), the Appeal Board listed five circumstances in which conduct not alleged in an SOR may be considered, stating:

> (a) to assess an applicant's credibility; (b) to evaluate an applicant's evidence of extenuation, mitigation, or changed circumstances; (c) to consider whether an applicant has demonstrated successful rehabilitation; (d) to decide whether a particular provision of the Adjudicative Guidelines is applicable; or (e) to provide evidence for whole person analysis under Directive Section 6.3.

Id. (citing ISCR Case No. 02-07218 at 3 (App. Bd. Mar. 15, 2004); ISCR Case No. 00-0633 at 3 (App. Bd. Oct. 24, 2003)). *See also* ISCR Case No. 12-09719 at 3 (App. Bd. Apr. 6, 2016) (citing ISCR Case No. 14-00151 at 3, n. 1 (App. Bd. Sept. 12, 2014); ISCR Case No. 03-20327 at 4 (App. Bd. Oct. 26, 2006)). The non-SOR allegations will not be considered except for the five purposes listed above.

Applicant demonstrated the correct attitude and commitment to security awareness. He was serious, candid, and credible at the hearing. He cooperated fully during his background investigation and throughout this process. Applicant, has matured since his first clearance denial. The added responsibility of being a parent has most likely contributed to his increased maturity. Applicant is an involved and engaged parent for his two minor children. No doubt this experience has been a teachable moment for Applicant. He is committed to following all rules and regulations pertaining to security awareness.

I take this position based on the law, as set forth in *Department of Navy v. Egan,* 484 U.S. 518 (1988), my careful consideration of the whole-person factors and supporting evidence, my application of the pertinent factors under the adjudicative process, and my interpretation of my responsibilities under the adjudicative guidelines.

Formal Findings

The formal findings on the SOR allegations are:

Paragraph 1, Guideline M:	For Applicant
Subparagraphs 1.a – 1.d:	For Applicant
Paragraph 2, Guideline K:	For Applicant
Subparagraph 2.a:	For Applicant

Conclusion

In light of the record as a whole, it is clearly consistent with the national interest to grant Applicant eligibility for a security clearance. National security eligibility is granted.

_____
Robert Tuider
Administrative Judge