DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 19-02413)
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Jeff Nagel, Esq., Department Counsel
For Applicant: Alan V. Edmunds, Esq.

05/11/2022

_____

Decision

_____

COACHER, Robert E., Administrative Judge:

Applicant mitigated the security concerns Guideline K, handling protected information. Guideline E was not applicable under the established facts. Applicant's eligibility for a security clearance is granted.

Statement of the Case

On February 26, 2020, the Department of Defense (DOD) issued Applicant a Statement of Reasons (SOR) detailing security concerns under Guidelines K and E. The DOD acted 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) implemented by the DOD on June 8, 2017.

Applicant answered the SOR on March 27, 2020, and requested a hearing. The case was assigned to me on October 21, 2021. The Defense Office of Hearings and

Appeals (DOHA) issued a notice of hearing on November 8, 2021, and the hearing was held as scheduled on December 17, 2021. The Government offered exhibits (GE) 1 through 5, which were admitted into evidence without objection. The Government's exhibit list was marked as hearing exhibit (HE) I. Applicant testified, called one witness, and offered exhibits (AE) A-L, which were admitted without objection. His exhibit list was marked as HE II. DOHA received the hearing transcript (Tr.) on December 30, 2021.

Findings of Fact

Applicant admitted all the SOR allegations with explanations and clarifications. His admissions are adopted as findings of fact. After a thorough and careful review of the pleadings and exhibits submitted, I make the following additional findings of fact.

Applicant is 44 years old. He has worked for a defense contractor for approximately 18 years. He holds a master's degree. He is married and has six children, ages 15, 14, 10, 8, 6, and 4. He has held a security clearance for 17 years. (Tr. 31, 33; GE 1)

The allegations are relatively straightforward and the facts are not in dispute. The SOR cites seven separate security lapses under Guideline K as follows: (1) in March 2007, Applicant installed an unauthorized memory upgrade chip onto his work computer; (2) in October 2012, he brought a personal cell phone into a sensitive compartmented information facility (SCIF); (3) in November 2013, he removed hand-written notes from a SCIF, that were thought to be classified, but turned out not to be classified; (4) In May 2015, he failed to completely lock a security container at the end of the day; (5) in October 2015, he failed to re-file classified information and to lock the security container at the end of the day; (6) in February, he removed classified information from the SCIF; and (7) in August 2018, he brought his personal cell phone into the SCIF. The exact allegations are cross-alleged under Guideline E. (SOR)

Applicant's explanation for each incident is as follows:

1. March 2007 incident. Applicant admitted this violation. It was unintentional. He was not aware that only the systems administrator could install new software or hardware onto his company computer. Applicant self-reported this violation once he realized that he was not authorized to do what he did. There was no compromise of classified information. (Tr. 26, 41, 44, 48; SOR answer; GE 4)

2. October 2012 incident. Applicant admitted this violation. It was unintentional. He realized he brought his cell phone into a secure area after about 40 minutes. Applicant immediately left the area and self-reported this violation. No calls were made or received while the phone was in the SCIF. There was no compromise of classified information. Applicant received verbal counseling. (Tr. 26, 41, 44, 48; SOR answer; GE 5)

3. November 2013 incident. Applicant admitted this violation. It was unintentional. He took notes on an index card while he was accessing classified

information. He left work for the day without realizing he had the index card in his pocket. Upon realizing he still possessed the card, he returned the card to his workplace and he reported the incident to security. Upon examination by security, it was discovered that no classified information was contained on the card itself. Applicant was directed to use a notebook with a classified coversheet to take notes. Applicant adopted this practice and still uses it to this day. He then leaves the notebook secured in the SCIF. (Tr. 26, 41, 44, 48; SOR answer; GE 5)

4. May 2015 incident. Applicant admitted this violation. It was unintentional. He closed the lock, but it did not fully engage. While the container was not properly secured, it remained in a secure area where only cleared or escorted people have access. Applicant immediately self-reported this violation. There was no compromise of classified information. Applicant received verbal counseling. (Tr. 26, 41, 44, 48; SOR answer; GE 5)

5. October 2015 incident. Applicant admitted this violation. It was unintentional. He was distracted at the end of the day by leadership issues he was addressing and neglected to complete his checklist, which resulted in classified material not being placed in a container and the container not being properly locked. While the container was not properly secured, it remained in a secure area where only cleared or escorted people have access. Applicant immediately self-reported this violation the following morning. There was no compromise of classified information. Applicant received refresher training. (Tr. 26, 41, 44, 48; SOR answer; GE 5)

6. February 2016 incident. Applicant admitted this violation. It was unintentional. He took a printout of his personal calendar out of the SCIF. He reviewed the printout while sitting in his car and realized it contained classified information. He immediately returned the printout to his office and placed it in a closed area. Applicant immediately self-reported this violation. There was no compromise of classified information. Applicant received verbal counseling. (Tr. 26, 41, 44, 48; SOR answer; GE 5)

7. August 2018 incident. Applicant admitted this violation. It was unintentional. He realized he brought his cell phone into a secure area. It was there for about 20 minutes before he realized he had it. No classified information was discussed while he possessed the cell phone. Applicant immediately left the area and self-reported this violation. No calls were made or received while the phone was in the SCIF. There was no compromise of classified information. Applicant was told to be more careful. (Tr. 26, 41, 44, 48; SOR answer; GE 5)

Applicant did not attempt to deflect or avoid responsibility for these security lapses. He accepted full responsibility for his security mistakes. Applicant works "hands-on" with classified information approximately 24 days a month, including multiple times a day. By way of explanation, Applicant described some events going on in his life during some of his earlier security violations. In 2013-2014, he had just assumed a leadership role in his company. One of his leadership tasks was to "fix" two broken

teams. There were significant personnel issues with these teams that he was trying to overcome. Additionally, in his personal life, he was going through a major home renovation, and his fourth and fifth children were born. His wife was hospitalized for three months before the birth of their fourth child because of a medical condition. This was a very stressful time for Applicant. (Tr. 34, 41-43)

Applicant described the changes he has made in his work routine to ensure that he follows all prescribed security protocols. He has not had a security violation in over three years. The changes he implemented include: consciously slowing down at the end of the day to ensure he follows all the proper closing procedures; following repetitive patterns, such as always putting his cell phone in the same place so it is easier to check to see if he still possesses it; at the end of the day, he closes his office door, thereby preventing outside distractions from interfering with his end-of-the-day security procedures. (Tr. 43-45)

Applicant's company continues to retain confidence in him. Applicant's immediate supervisor (Ms. L), who is a company vice president and who is responsible for several hundred employees and contractors, testified that Applicant is currently her deputy, acting in her place when she is unavailable. Ms. L has known Applicant for six years and he has been her deputy for two years. She is fully aware of all the Applicant's security incidents and the circumstances behind them. Ms. L believes that Applicant has unquestioned integrity as demonstrated by his self-reporting of every security incident. She also described the changes she observed in Applicant's security practices, e.g., he no longer takes notes when reviewing material in SCIF or if he does take notes he uses a notebook, which he ensures is secured before leaving the SCIF. Ms. L strongly believes Applicant is not a security risk and recommends that his security clearance access continue. She also provided a written letter of support. (Tr. 22-27, 36-37; AE A, E)

Applicant offered several letters of support from coworkers, church acquaintances, and his sister. The regional security manager for Applicant's company commented on Applicant's selection for an executive growth program and that he was a top performer. He also wrote about Applicant's security infractions, but also noted that Applicant always accepted responsibility and never made excuses. None of the incidents resulted in a compromise of classified information. He concluded his letter by stating: "I trust [Applicant] and do not question his loyalty to the United States of America." Three other coworkers also referenced Applicant's willingness to take responsibility for his security lapses and described his strong character traits of integrity, reliability, and trustworthiness. (AE A, E)

Applicant's church acquaintances describe Applicant's mentorship in youth programs and his willingness to help others. He is described as selfless and committed to helping others. His sister described Applicant as a man of integrity who is reliable and trustworthy. (AE E)

Applicant's job performance appraisals from 2013 to 2020 reflect that his ratings were "exceeded commitments" or "significantly exceeded commitments." Between 2005 and 2020, he was also the recipient of numerous company awards. (AE B, F, H)

Policies

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 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 commonsense decision. According to AG ¶ 2(a), the entire process is a careful weighing of a number of variables known as the "whole-person concept." The administrative judge must consider all available, reliable information about the person, past and present, favorable and unfavorable, in making a decision.

The protection of the national security is the paramount consideration. AG ¶ 2(b) requires that "[a]ny doubt concerning personnel being considered for national security eligibility will be resolved in favor of the national security." In reaching this decision, I have drawn only those conclusions that are reasonable, logical, and based on the evidence contained in the record.

Under Directive ¶ E3.1.14, the Government must present evidence to establish controverted facts alleged in the SOR. Under Directive ¶ E3.1.15, an "applicant is responsible for presenting witnesses and other evidence to rebut, explain, extenuate, or mitigate facts admitted by applicant or proven by Department Counsel, and 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 an applicant may deliberately or inadvertently fail to safeguard classified information. Such decisions entail a certain degree of legally permissible extrapolation about potential, rather than actual, risk of compromise of classified information.

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 expresses the security concern pertaining to handling protected information:

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

I have considered all the handling protected information disqualifying conditions under AG ¶ 34 and determined the following apply:

> (g) any failure to comply with rules for the protection of classified or other sensitive information; and
>
> (h) negligence or lax security practices that persist despite counseling by management.

Applicant had seven documented security incidents from 2007 to 2018. AG ¶¶ 34(a) and 34(g) apply.

All the mitigating conditions for handling protected information under AG ¶ 35 were considered and the following were found relevant under these circumstances:

> (a) so much time has elapsed since the behavior, or it has happened so infrequently or under such unusual circumstances, that it is unlikely to recur and does not cast doubt on the individual's current reliability, trustworthiness, or good judgment;
>
> (b) the individual responded favorably to counseling or remedial security training and now demonstrates a positive attitude toward the discharge of security responsibilities; and
>
> (d) the violation was inadvertent, it was promptly reported, there is no evidence of compromise, and it does not suggest a pattern.

Applicant's has not had a security violation since August 2018. He is someone who is exposed to classified information on an almost daily basis. While his previous security incidents are certainly concerning, both he and his supervisor described his changed security practices, which have prevented recurrences in the last three years. All the incidents were inadvertent, there was no compromise of classified information, and Applicant immediately reported each incident as soon as he became aware of the violation. Both his current supervisor and the company security manager support his

continued access to classified information. All the above mitigating circumstances substantially apply.

Guideline E, Personal Conduct

AG ¶ 15 expresses the personal conduct security concern:

> 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.

AG ¶ 16: Conditions that could raise a security concern and may be disqualifying include:

> (c) credible adverse information in several adjudicative issue areas that is not sufficient for an adverse determination under any other single guideline, but which, when considered as a whole, 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;
>
> (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.
>
> (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.

This case is strictly about Applicant's handling of classified information and following proper security procedures, which is specifically covered by Guideline K (AG ¶¶ 34-35). Additionally, Applicant's inadvertent actions and immediate self-disclosure do not rise to a concern level as contemplated by AG ¶ 16(e). None of the disqualifying conditions under AG ¶ 16 apply.

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 considered Applicant's multiple security violations over an extended time. However, I also considered the inadvertent nature of the violations, Applicant's self-reporting, taking responsibility for his violations, his dedication to making changes to his security practices, and the support of his supervisor, security manager, other coworkers and acquaintances. Applicant provided sufficient evidence to mitigate the handling protected information security concerns. Personal conduct security concerns were not established.

Overall the record evidence leaves me without questions or doubts about Applicant's eligibility and suitability for a security clearance. For all these reasons, I conclude Applicant mitigated the security concerns under Guideline K and no independent security concerns were established under Guideline E.

Formal Findings

Formal findings for or against Applicant on the allegations set forth in the SOR, as required by section E3.1.25 of Enclosure 3 of the Directive, are:

Paragraph 1, Guideline K:	FOR APPLICANT
Subparagraphs 1.a – 1.g:	For Applicant
Paragraph 2, Guideline E:	FOR APPLICANT
Subparagraph 2.a:	For Applicant

Conclusion

In light of all of the circumstances presented by the record in this case, it is clearly consistent with the national interest to grant Applicant eligibility for a security clearance. Eligibility for access to classified information is granted.

_____

Robert E. Coacher
Administrative Judge