DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
REDACTED	)	ISCR Case No. 15-05533
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Nicole A. Smith, Esq., Department Counsel
For Applicant: Alan V. Edmunds, Esq.

05/23/2017

Decision

MENDEZ, Francisco, Administrative Judge:

Applicant mitigated security concerns raised by her inadvertent, minor security lapses that occurred three years ago. She self-reported the incidents and took corrective action. These security infractions were an aberration in an otherwise long history of properly handling and safeguarding classified, sensitive, and proprietary information. Applicant established that similar security incidents are unlikely to recur. She did not falsify her security clearance application. Clearance is granted.

Statement of the Case

On February 21, 2016, the Department of Defense (DOD) Consolidated Adjudications Facility (CAF) sent Applicant a Statement of Reasons (SOR) alleging security concerns under Guideline K (handling protected information) and Guideline E (personal conduct).[1] Applicant answered the SOR and initially requested a decision on the written record. She subsequently requested a hearing to establish her eligibility for continued access to classified information.

[1] This action was taken under Executive Order (E.O.) 10865, *Safeguarding Classified Information within Industry* (February 20, 1960), as amended; Department of Defense Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (January 2, 1992), as amended (Directive); and the Adjudicative Guidelines (AG) implemented by the Department of Defense on September 1, 2006.

On April 11, 2017, a date mutually agreed to by the parties, a hearing was held. Applicant testified and called two witnesses, a character reference and a co-worker. Both sides offered exhibits, which were admitted into the administrative record without objection. (Government Exhibits 1 – 3; and Applicant's Exhibits A – K.)[2] The transcript of the hearing was received on April 19, 2017, and the record closed on May 5, 2017.

Findings of Fact

General Background[3]

Applicant, 55, is the granddaughter of refugees who fled a brutal genocide and immigrated to the United States. She was born, raised, and educated in the United States. She has been married to her husband for nearly 35 years. They adopted their two children, one of whom suffers from learning and physical disabilities.

Applicant holds a master's degree in mechanical engineering and earned an advanced degree in management from a prestigious U.S. business school. She is an executive at her company, a federal contractor. Her position with the company is primarily in the business development arena, though her portfolio is quite extensive. She is the person others in the company seek out for advice and she is often asked to handle and resolve the most challenging issues – assignments that she routinely accepts. She has been highly successful at her job, generally exceeding expectations and regularly earning six-figure bonuses. She has received repeated promotions over the years, with ever increasing responsibilities and demands.

In the past five years, Applicant has been selected as the chair of a select industry trade group; named by a U.S. publication as one of the top five women in her (traditionally male-dominated) field; and invited as a guest speaker at a high-visibility U.S. military forum. She mentors young female executives at her company. In July 2015, she was promoted to her current vice president position. She has been with her current employer since 1989, and has held a clearance since at least 1999.

When not at work, Applicant helps care for her elderly parents and is active in her community. Through her church, Applicant volunteers mentoring teenage girls from disadvantaged backgrounds. She became involved in this charitable endeavor about ten years ago, after returning from a church-sponsored mission trip to a war-torn, third-world country where her children were born.

The director of the church's youth ministry, who has known Applicant for about a decade, testified at the hearing. He states that Applicant is a great role model of the values his ministry tries to instill in young people of "Integrity, Courage, Honesty,

[2] Applicant's request for hearing, prehearing correspondence, the notice of hearing, case management order are attached to record as Appellate Exhibits (App. Exh.) I – IV, respectively.

[3] Unless otherwise indicated, the pertinent portions of the record that were primarily relied upon for the information relayed in this section can be found at Tr. 9-45, 52-53; Exhibit 1; Exhibits A - K.

Discipline, Determination, and Strength." He also states that Applicant "is a person of the highest integrity. You would have to go a long way to find someone with greater moral character."[4] Other individuals, including the president of her company and a fellow youth minister, provided similar glowing accolades.

Security Infractions[5]

In 2014, Applicant's work office also doubled as a sensitive compartmented information facility (SCIF). The company's senior security officer (SSO) provided a letter noting some inherent issues with the SCIF's setup at the time that "increased the opportunity for inadvertent security infractions, particularly with prohibited electronic devices."[6] The unique issues identified by the security manager and Applicant's executive assistant, a 20-year military veteran, were as follows:

1. The SCIF was a stand-alone secure office with only one exterior door, which was permitted to remain open as long as the executive assistant or Applicant were present and no discussion of classified information was occurring.

2. The SCIF did not have an anteroom (or "mantrap") with a locker or other suitable container that would allow a person entering the SCIF to place their personal belongings, cell phone, and other electronic equipment. As soon as a person crossed the threshold of the office door, which at times was propped open, that person was in a secure environment.

3. The company issued Applicant a laptop that she could use within the SCIF to work on classified and non-classified matters. She was also issued a wireless card that she could use with the laptop outside the SCIF.

The Government approved the setup of the SCIF (Applicant's office) and Applicant's use of a company laptop, which could be connected to the internet through the company-provided removable wireless card when she was not working in the SCIF.

In about January 2014, Applicant requested that a locker or other suitable container be placed outside the SCIF to lessen the risk of an inadvertent security violation. Her supervisor at the time initially denied the request. She eventually was able to convince upper management to get a locker placed outside the office door, which she and her executive assistant could then use to place their purses, brief cases, cell phone, and other non-classified electronic equipment. The locker did not arrive until late 2014, as the responsible company representative searched for one that would match the style of the furniture in other executive office suites.

[4] Tr. 9-15; Exhibit J.

[5] Unless otherwise indicated, the pertinent portions of the record that were primarily relied upon for the information relayed in this section can be found at Tr. 18-33, 45-60; Exhibits 1-3; Exhibit J at 1, 7-9.

[6] Exhibit J at 8.

Applicant's executive assistant testified that in 2014, Applicant had a very busy schedule and was inundated with a number of job-related tasks outside her primary area of responsibility. Applicant would routinely walk in and out of her office (SCIF) throughout the day to attend meetings. She was also provided a laptop by the company, which she could carry in and out of her office (SCIF), from and to her home, and while on business-related travel. She had to remember to remove the wireless card before entering her office (SCIF).

During a busy six-month period from late winter to early summer of 2014 Applicant had several successive security infractions involving the unauthorized introduction of electronic devices into her office (SCIF). In February 2014, following a round of business meetings, she was carrying a stack of papers in her hands from a recent presentation. In the stack was the company-issued wireless card and her smart phone. She carried the stack into her office (SCIF). The wireless card was not connected to the laptop or any other electronic device. A company president, whose office was next to Applicant's, writes that he saw Applicant run out of the SCIF within seconds of recognizing what she had done and immediately reported the matter to company security. These incidents are alleged at SOR 1.a and 1.b.

In June 2014, Applicant was given a temporary, loaner laptop by her employer while her usual company-issued laptop was being upgraded. This loaner laptop, however, was not approved for use in the SCIF (her office). She mistakenly brought the loaner laptop into her office. This incident is referenced at SOR 1.c. In early July 2014, Applicant returned from a business trip and did not clean out the computer bag she used on the trip. She brought the computer bag into her office (SCIF) the following Monday, with the company-issued wireless card still in its plastic sleeve inside the computer bag. The wireless card was not connected to the laptop or any other electronic device. This incident is referenced at SOR 1.d.

Applicant testified that she self-reported these security incidents to her security office.[7] This is corroborated by Applicant's executive assistant, her supervisor at the time, and the company's senior security officer (SSO).[8] The security office and the Government client determined that each of the incidents constituted an infraction. An "infraction" is "[a] failure to follow proper security procedures that does or is not likely to result in a compromise of classified information."[9] However, due to internal corporate policy at the time, the incidents were collectively deemed a violation. Nevertheless, company security and the Government client "did not suspect a compromise of classified information." This corporate policy has since been changed to allow the

[7] Tr. 51.

[8] Exhibit 2; Exhibit J at 7-8. In assessing the weight to extend to the testimony and statements of other company employees, I have considered the potential for bias as Applicant is a high performer for the company (having generated over $100 million in profits for the company in one year alone). However, no evidence of unlawful collusion was presented or evident from the record. Furthermore, after considering the entire record evidence, I found the information provided by these individuals credible.

[9] Exhibit J at 8.

responsible security officials to assess whether a group of incidents rise to the level of a violation.[10]

In late July 2014, Applicant and her supervisor had a meeting to discuss the security incidents and potential ways to avoid a recurrence of the issue. He gave Applicant a letter for reprimand (LOR), which states in pertinent part:

> You are hereby reprimanded. Everyone makes mistakes; however this is becoming a pattern. While I view these incidents as oversights and not a negligent disregard for security procedures, my expectation is that you, as a seasoned executive with extensive background in supporting classified programs will be able to correct this. I have full confidence that you will.[11]

Applicant's security clearance eligibility and access to classified information was not suspended or revoked. She was also not offered any remedial security training after any of the incidents or the reprimand. She was not notified, either formally or informally, that the security infractions amounted to employee misconduct. Less than a year later, Applicant was promoted and given additional responsibilities and duties, to include handling highly sensitive U.S. Government information.

Following the security incidents, Applicant placed signs outside her office to remind herself and others to remove and secure all electronic equipment before entering her office space (the SCIF). Since the July 2014 security incident, Applicant has not been involved in any such incidents.

Sometime after the LOR was issued, the company installed a cabinet or locker outside Applicant's (former) office. Persons now entering the office (SCIF) can put their personal belongings and electronic equipment in a secure container. The company also stopped issuing non-secured laptops to those working in classified environments and installed a desktop in the SCIF.

The SSO notes that Applicant's "track record prior to and after this series of incidents has been solid." He also states that he has frequent interaction with Applicant and the incidents themselves do not change his opinion as to her trustworthiness, reliability, and good judgment.[12]

[10] Exhibit J at 8.

[11] Exhibit 2.

[12] Exhibit J at 8.

Personal Conduct[13]

Applicant completed a security clearance application (SCA) in October 2014. Section 13.C, *Employment Record*, of the SCA asks:

> Have any of the following happened to you **in the last seven (7) years** at employment activities that you have not previously listed? . . .
>
> - Fired from a job?
> - Quit a job after being told you would be fired?
> - Have you left a job by mutual agreement following charges or allegations of misconduct?
> - Left a job by mutual agreement following notice of unsatisfactory performance?
> - Received a written warning, been officially reprimanded, suspended, or disciplined for misconduct in the workplace, such as violation of a security policy?

Applicant answered "No" to this question.[14] A few months later, during a security clearance interview, Applicant volunteered the information about the security incidents and the reprimand.[15]

At hearing, Applicant explained that she answered the workplace misconduct question in the manner she did, because she did not consider the reprimand an official or even unofficial negative mark in her employment record. She was not formally notified or even informally told that her conduct rose to the level of workplace misconduct. She is familiar with the corporate forms used to notify an employee that their conduct constitutes workplace misconduct or is deficient in some manner. Her supervisor did not use any of these forms during or after the meeting.

Applicant's executive assistant, who has held a clearance and been involved with highly-classified projects as both a federal contractor and military member for the past 20 years, assisted Applicant in filling out her SCA by the deadline set by corporate

[13] Unless otherwise indicated, the pertinent portions of the record that were primarily relied upon for the information relayed in this section can be found at Tr. 23-34, 45-60; Exhibits 1-2; Exhibit J at 7.

[14] Exhibit 1 at 11. The SCA at issue does not contain a specific question asking an applicant to disclose if they were ever involved or found to have committed a security infraction or violation. Instead, the SCA only asks an applicant to disclose situations where their clearance was suspended, denied, or revoked. Exhibit 1 at 44. The only question that presumably asks an applicant to disclose a security infraction or violation, as alleged in the SOR, is in Section 13.C, a section that is clearly tailored to find about any adverse employment history, including workplace misconduct. Based on this context, the question at issue appears to be asking an applicant to reveal security incidents involving violence or other unlawful conduct, not an incident involving the oversight of a rule or regulation for the protection of protected information. However, this issue is somewhat moot in light of my finding that Applicant did not deliberately falsify her SCA nor attempted to mislead the Government about this information.

[15] Exhibit 3 at 2.

security. At the time, the executive assistant was aware that Applicant had committed the security infractions and of the LOR's existence. She reviewed the SCA and did not believe the information about the security infractions or LOR needed to be listed on the SCA. She noted that the Government client was fully aware of the security infractions well before the SCA was submitted, because she (Applicant) had self-reported the information to corporate security. Applicant and the executive assistant's testimony was credible, reasonable, and fully consistent with the other record evidence.

Policies

"[N]o one has a 'right' to a security clearance." *Department of the Navy v. Egan*, 484 U.S. 518, 528 (1988). Individual applicants are eligible for access to classified information "only upon a finding that it is clearly consistent with the national interest" to authorize such access. E.O. 10865 § 2.

When evaluating an applicant's eligibility for a security clearance, an administrative judge must consider the adjudicative guidelines (AG). In addition to brief introductory explanations, the guidelines list potentially disqualifying and mitigating conditions. The guidelines are not inflexible rules of law. Instead, recognizing the complexities of human behavior, an administrative judge applies the guidelines in a commonsense manner, considering all available and reliable information, in arriving at a fair and impartial decision.

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

Administrative Judges are responsible for ensuring that an applicant receives fair notice of the issues raised, has a reasonable opportunity to litigate those issues, and is not subjected to unfair surprise. ISCR Case No. 12-01266 at 3 (App. Bd. Apr. 4, 2014). In resolving the ultimate question regarding an applicant's eligibility, an administrative judge must resolve "[a]ny doubt concerning personnel being considered for access to classified information . . . in favor of national security." AG ¶ 2(b). Moreover, recognizing the difficulty at times in making suitability determinations and the paramount importance of protecting national security, the Supreme Court has held that "security clearance determinations should err, if they must, on the side of denials." *Egan*, 484 U.S. at 531.

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. 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 an 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.

Analysis

Guideline K, 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.[16]

Security clearance cases require administrative judges to assess whether an applicant has the requisite good judgment, reliability, and trustworthiness to be entrusted with classified information. When evidence is presented that an applicant previously mishandled classified information or violated a rule or regulation for the protection of protected information such an applicant bears a very heavy burden in demonstrating that they should once again be found eligible for a security clearance.[17]

Applicant's commission of four security incidents in a relatively short time span raise the overall Guideline K security concern. In assessing Applicant's case, I considered the following pertinent disqualifying and mitigating conditions:

> AG ¶ 34(g): any failure to comply with rules for the protection of classified or other sensitive information;

> AG ¶ 35(a): so much time has elapsed since the behavior, or it happened so infrequently or under such unusual circumstances that it is unlikely to recur or does not cast doubt on the individual's current reliability, trustworthiness, or good judgment; and

> AG ¶ 35(b): the individual responded favorably to counseling or remedial security training and now demonstrates a positive attitude toward the discharge of security responsibilities.

The incidents at issue occurred three years ago. However, the passage of time alone, without evidence of true reform and rehabilitation, is insufficient to mitigate the heightened security concerns at issue. Instead, the focus of the inquiry is whether the person has: (1) accepted responsibility for the incident(s), (2) reformed the behavior that led to or contributed to the incident(s), and (3) established that a similar incident(s) is

[16] AG ¶ 33.

[17] ISCR Case No. 11-12202 at 5 (App. Bd. June 23, 2014) (very heavy burden standard); ISCR Case No. 01-25941 at 5 (App. Bd. May 7, 2004) (security clearance determinations are "not an exact science, but rather predicative judgments.").

(are) unlikely to recur. A judge must review any claim of reform and rehabilitation with "strict scrutiny."[18] Applicant met this burden.

Applicant's past security lapses were not deliberate nor the result of a reckless or even negligent disregard for security rules and regulations.[19] Instead, the major contributing factors were personal inattentiveness and working in a unique environment that lacked the usual safeguards to help prevent the inadvertent security lapses that occurred. Of note, despite Applicant's warnings and attempts to remedy the situation, Applicant's employer and the Government allowed the inherent vulnerability issues with the SCIF to continue, even after the first few incidents.

Applicant fully acknowledges her responsibility for the incidents. She self-reported them, which allowed the responsible security officials to review the situation and determine that no compromise occurred.[20] She then responded favorably to the counseling with her supervisor and took corrective action to put in place the proper safeguards to avoid a recurrence of a similar incident. She has not been involved in any type of security incident in the past three years. Rather, over the past three years, she has properly handled and safeguarded closely guarded U.S. and corporate information. Before these incidents, she had a long track record of properly handling and safeguarding protected information. AG ¶¶ 35(a) and 35(b) apply.

Additionally, the significant and overwhelming whole-person evidence adduced at hearing clearly establishes that Applicant has and exhibits the good judgment, reliability and trustworthiness expected of all clearance holders. Therefore, I am firmly convinced that Applicant will continue to properly discharge her security responsibilities and that the security lapses at issue were an aberration.[21]

Guideline E, Personal Conduct

The SOR alleges Applicant deliberately falsified her SCA by not disclosing the security infractions and LOR in response to the question about workplace misconduct. The deliberate falsification of a SCA raises the personal conduct security concern, which is explained at AG ¶ 15:

---

[18] ISCR Case No. 06-21537 at 4 (App. Bd. Feb. 21, 2008).

[19] *Contrast with* ISCR Case No. 07-08119 at 5 (App. Bd. July 8, 2010) ("ongoing pattern of knowing and willful security violations").

[20] *Contrast with* ISCR Case No. 06-21537 (favorable decision undermined by determination that actual compromise occurred and applicant's failure to take responsibility for their conduct).

[21] *See generally* ISCR Case No. 04-05802 at 3-4 (App. Bd. Jun. 13, 2007) (Board affirmed favorable decision where applicant had committed seven security violations in a short period of time, because the judge's findings "concerning the impact that Applicant's workload had upon his mistakes; the inadvertent nature of the violations; . . . and steps Applicant has taken to ensure his compliance with security procedures," as well as "the Judge's evaluation of Applicant as a believable and honest witness in his own behalf" were supported by the record evidence).

> 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 information. Of special interest is any failure to provide truthful and candid answers during the security clearance process or any other failure to cooperate with the security clearance process.

The security clearance process is contingent upon the candor of all applicants. It begins with the answers provided in the SCA and continues throughout the security clearance process. However, the omission of material, adverse information standing alone is not enough to establish that an applicant intentionally falsified his or her SCA. An omission is not deliberate if the person genuinely forgot the information requested, inadvertently overlooked or misunderstood the question, or sincerely thought the information did not need to be reported. An administrative judge must examine the facts and circumstances surrounding the omission to determine an applicant's true intent.[22]

Applicant did not deliberately falsify her SCA. She self-reported the security incidents when they occurred to the Government through her employer's security office. She then volunteered the information during her clearance interview. Applicant's conduct is inconsistent with the expected actions of a person who is attempting to hide or mislead the Government. Instead, by reporting the security incidents and freely volunteering the information during her clearance interview, Applicant showed that she can be trusted to place her security obligations over her own personal concerns or interests. Furthermore, I found her testimony that she did not believe the security infractions and reprimand needed to be listed on the SCA credible, reasonable, and consistent with other record evidence.

After a complete and thorough review of the record evidence, while remaining mindful of my solemn obligation to resolve any unmitigated doubt in favor of protecting national security, I find that Applicant met her burden of proof and persuasion in mitigating or refuting the security concerns at issue. Furthermore, she clearly established her eligibility for continued 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 (Handling Protected Information):	FOR APPLICANT
Subparagraphs 1.a – 1.e:	For Applicant
Paragraph 2, Guideline E (Personal Conduct):	FOR APPLICANT
Subparagraph 2.a:	For Applicant

[22] *See generally* ISCR Case No. 02-12586 (App. Bd. Jan. 25, 2005).

Conclusion

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

_____
Francisco Mendez
Administrative Judge