DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
----------	)	ISCR Case No. 17-02211
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Adrienne Driskill, Esq., Department Counsel
For Applicant: *Pro se*

11/26/2018

Decision

LEONARD, Michael H., Administrative Judge:

Applicant contests the Defense Department's intent to revoke his eligibility for access to classified information. He was involved in six security incidents from April 2014 to February 2016. Four of the six incidents resulted in a determination that he was culpable or a responsible party. Two of the incidents were still pending a determination at the time of the April 2018 hearing. He has had no further security incidents since February 2016. The evidence is not sufficient to mitigate the serious security concern stemming from his involvement in the six security incidents. Accordingly, this case is decided against Applicant.

Statement of the Case

Applicant completed and submitted a Standard Form (SF) 86, Questionnaire for National Security Positions, on October 8, 2015.[1] It is the official form that military personnel, federal contractors, and federal employees complete in order for the

[1] Exhibit 1.

Government to collect information for conducting background investigations, reinvestigations, and continuous evaluations of people under consideration for, or retention of, national security positions. It is commonly known as a security clearance application.

On September 12, 2017, after reviewing the application and the information gathered during a background investigation, the Department of Defense Consolidated Adjudications Facility, Fort Meade, Maryland, sent Applicant a statement of reasons (SOR), explaining it was unable to find that it was clearly consistent with the national interest to grant him eligibility for access to classified information. The SOR is similar to a complaint. It alleged the factual reasons—Applicant's involvement in six security incidents—under the security guideline known as Guideline K for handling protected information. In addition, the SOR cross-alleged the six security incidents under Guideline E for personal conduct. And the SOR cross-alleged two of the security incidents, which involved a process called assured file transfer, under Guideline M for use of information technology.

Applicant answered the SOR on September 20, 2017. He admitted his involvement in the six security incidents and provided an explanation for each. He also requested a hearing before an administrative judge.

The case was assigned to me on November 7, 2017. The hearing took place as scheduled on April 12, 2018. Applicant appeared without counsel. Department Counsel offered documentary exhibits, which were admitted as Exhibits 1 and 3; Exhibit 2 was not admitted based on Applicant's objection. Applicant's documentary exhibits were admitted as Exhibits A-E. Other than Applicant, no witnesses were called by either party. The record was kept open until April 30, 2018, to allow Applicant to present letters of reference or recommendation. He timely submitted three such letters, and they are admitted without objections as Exhibits F, G, and H.

Findings of Fact

Applicant is a 42-year-old engineer logistics specialist who is seeking to retain a top-secret security clearance. His first marriage ended in a divorce. He has two minor children from that marriage. He married for the second time in 2011. His formal education includes a bachelor's degree in criminal justice. He has worked for his current employer since April 2001. He was initially granted a security clearance at the secret level in 2002, and was granted a top-secret security clearance in 2011. He has a very good employment record according to three co-workers who submitted letters of recommendation on his behalf.[2] Those people regard Applicant as an honest and ethical person of integrity who is a valued employee.

As alleged in the SOR, the evidence establishes that Applicant was involved in six security incidents from April 2014 to February 2016.[3] Four of the six incidents

[2] Exhibits F, G, and H.

[3] Exhibit 3.

resulted in a determination that he was culpable or the responsible party. Two of the incidents were pending a final determination at the time of the April 2018 hearing. He has had no further security incidents since February 2016. The six security incidents are discussed below.

The first incident occurred in April 2014, when Applicant was faulted for failure to properly respond to an alarm leaving a classified area unattended overnight after being notified that the alarm was not operational.[4] He received a security infraction as a result. Applicant explained that he received a telephone call from his employer's dispatcher that an employee was intending to depart with an alarm unarmed due to technical problems; he advised the employee to double-check all doors, which they had done; he then advised the employee to have the dispatcher contact the security company responsible for the alarm system, but that was unsuccessful; and he then called the on-call technician for the alarm company who informed Applicant he would be unable to respond until the following morning at 8:00 AM. Faced with these circumstances, Applicant decided not to respond in-person because he had alcohol with dinner and did not want to drive. Instead, after assuring himself that the area was locked and secured, he requested that the room be checked by the security detail every hour instead of the normal two-hour check. His employer faulted him because this particular secured area was not available for a one-hour check. Although the alarm was not operational, the area was secured at all times and there was no compromise of classified or sensitive information.

The second incident occurred in February 2015, when Applicant was faulted for failing to properly secure a container.[5] He received an administrative action known as a practice detrimental to security (PDS), which is not a security infraction or violation, but an event, action, or behavior that could lead to a possible compromise of classified or sensitive information; a PDS can be delivered as an oral or written warning and is an opportunity for reeducation. The incident occurred when the middle drawer of a five-drawer container was left slightly cracked open in a secured area that was secured throughout. The incident occurred due to oversight. There was no compromise of classified or sensitive information.

The third incident occurred in April 2015, when Applicant was faulted for failing to properly secure an unclassified accreditation letter or document in the work area overnight.[6] He received a second PDS as a result. The incident occurred when he left the document in a courier bag outside of his desk area as opposed to placing the document in the secured container. Although he removed other documents from the bag and placed them in the secured container, the document in question was inadvertently left behind. There was no compromise of classified or sensitive information. As a result of this incident, Applicant's practice now is to place the courier

[4] Tr. 32-37.

[5] Tr. 37-43.

[6] Tr. 43-48.

bag in the secured container at the end of the day, thereby eliminating the risk of recurrence of a similar mistake.

The fourth and fifth incidents in October 2015 and February 2016, respectively, are similar in that Applicant was involved via his role in a process known as an assured file transfer (AFT).[7] As I understand it, this process is a risk-managed data transfer within the employer's special programs.[8] Applicant's role was that of the contract program security officer (CPSO), which required him to oversee the entire process; the CPSO is ultimately responsible to approve releasing all media containing "screened and cleaned" information; and the CPSO is responsible for obtaining and maintaining key (dirty word) lists. Applicant worked with subject-matter experts (SME) in this process; the SME are thoroughly knowledgeable of all aspects of a program, to include the involved technologies; and each SME is ultimately responsible to review all data intended for transfer and purge it of any non-releasable information. Further, each SME may be held liable for any security incidents or data spills that occur as the result of a properly executed transfer process but still results in a data spill due to improper data review.

According to the initial reports, for the October 2015 AFT, Applicant was faulted for using the wrong policy setting in a tool during the execution of an AFT, which resulted in the release and potential compromise of non-technical but classified program material.[9] For the February 2016 AFT, he was faulted for not following the approved AFT process using a particular tool, which resulted in the release and potential compromise of controlled program material.[10] The initial reports also state that a determination of security infraction versus security violation was pending. At the hearing, Applicant stated that he has not been disciplined for either incident.[11] Further, he understands the second incident was considered closed in March 2018, and that the parties involved were issued a PDS warning, although he did not received a PDS warning or any other type of warning or counseling.[12]

The sixth incident occurred in February 2016, when Applicant was faulted for briefing two employees for a program for which they were not vetted, resulting in the unauthorized disclosure of classified or sensitive information.[13] He received a security violation as a result, and he was suspended without pay for one week. The incident

[7] Tr. 54-68.

[8] Exhibit A.

[9] Exhibit 3.

[10] Tr. 43-48.

[11] Tr. 60.

[12] Tr. 65-66.

[13] Tr. 48-54.

occurred when he misread an approval letter, which led to the inadvertent disclosure to the two employees, which then had to be remediated.

On the day of the last incident, Applicant was removed from the program to which he was assigned and reassigned to another program.[14] He no longer performs AFT duties. He has had no further security incidents since the last incident in February 2016. He attributes his involvement in six security incidents during a two-year period (April 2014-February 2016) to a heavy workload, the press of business, and lack of sufficient attention to his duties.[15]

Law and Policies

This case is adjudicated 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 *National Security Adjudicative Guidelines for Determining Eligibility for Access to Classified Information or Eligibility to Hold a Sensitive Position* (AG), effective June 8, 2017.[16]

It is well-established law that no one has a right to a security clearance.[17] As noted by the Supreme Court in *Department of the Navy v. Egan*, "the clearly consistent standard indicates that security clearance determinations should err, if they must, on the side of denials."[18] Under *Egan*, Executive Order 10865, and the Directive, any doubt about whether an applicant should be allowed access to classified information will be resolved in favor of protecting national security. In *Egan*, the Supreme Court stated that the burden of proof is less than a preponderance of evidence.[19] The Appeal Board has followed the Court's reasoning, and a judge's findings of fact are reviewed under the substantial-evidence standard.[20]

A favorable clearance decision establishes eligibility of an applicant to be granted a security clearance for access to confidential, secret, or top-secret information.[21] An

[14] Tr. 68-69.

[15] Tr. 69-70.

[16] The 2017 AG are available at http://ogc.osd.mil/doha.

[17] *Department of the Navy v. Egan*, 484 U.S. 518, 528 (1988) ("it should be obvious that no one has a 'right' to a security clearance"); *Duane v. Department of Defense*, 275 F.3d 988, 994 (10th Cir. 2002) (no right to a security clearance).

[18] 484 U.S. at 531.

[19] 484 U.S. at 531.

[20] ISCR Case No. 01-20700 (App. Bd. Dec. 19, 2002) (citations omitted).

[21] Directive, ¶ 3.2.

unfavorable clearance decision (1) denies any application, (2) revokes any existing security clearance, and (3) prevents access to classified information at any level.[22]

There is no presumption in favor of granting, renewing, or continuing eligibility for access to classified information.[23] The Government has the burden of presenting evidence to establish facts alleged in the SOR that have been controverted.[24] An applicant is responsible for presenting evidence to refute, explain, extenuate, or mitigate facts that have been admitted or proven.[25] In addition, an applicant has the ultimate burden of persuasion to obtain a favorable clearance decision.[26]

Discussion

Under Guideline K, both willingness and ability to comply with rules and regulations for handling protected information are of central importance to an applicant's eligibility for access to classified information. The overall concern is:

> Deliberate or negligent failure to comply with rules and regulations for handling protected information—which includes classified information and other sensitive government information, and propriety information—raises doubt about an individual's trustworthiness, judgment, reliability, or willingness and ability to safeguard such information, and is a serious security concern.[27]

In addition to the concern under Guideline K, the Appeal Board has established a long line of caselaw concerning applicants who commit security infractions or violations. The central points of that caselaw are: (1) once it is established that an applicant has committed security violations or infractions, they have a "very heavy burden" of persuasion as to mitigation; (2) such violations or infractions "strike at the heart of the industrial security program;" and (3) any claims of reform or rehabilitation are viewed with "strict scrutiny."[28] Put differently, security infractions and violations are serious business, and they are not to be taken lightly.

In analyzing the facts of this case, I considered the following disqualifying and mitigating conditions as most pertinent:

---

[22] Directive, ¶ 3.2.

[23] ISCR Case No. 02-18663 (App. Bd. Mar. 23, 2004).

[24] Directive, Enclosure 3, ¶ E3.1.14.

[25] Directive, Enclosure 3, ¶ E3.1.15.

[26] Directive, Enclosure 3, ¶ E3.1.15.

[27] AG ¶ 33.

[28] *E.g.*, ISCR Case No. 15-04340 at 3 (App. Bd. Jan. 30, 2017) (citation omitted).

> AG ¶ 34(a) deliberate or negligent disclosure of protected information to unauthorized persons, including, but not limited to, personal or business contacts, the media, or persons present at seminars, meetings, or conferences;
>
> AG ¶ 34(g) any failure to comply with rules for the protection of classified or sensitive information;
>
> AG ¶ 34(h) negligence or lax security practices that persist despite counseling by management;
>
> AG ¶ 35(a) so much time has elapsed since the behavior, or it has happened so infrequently or under such unusual circumstances, that is it unlikely to recur and does not cast doubt on the individual's current reliability, trustworthiness, or good judgment; and
>
> AG ¶ 35(d) the violation was inadvertent, it was promptly reported, there is no evidence of compromise, and it does not suggest a pattern.

Applicant's involvement in six security incidents within a two-year period during 2014-2016 establish a pattern of negligence or laxness or both. The above disqualifying conditions apply. With that said, I have given less weight to the two incidents involving the AFT process because there has not been a final determination concerning Applicant's liability as well as the fact that others may have been held ultimately liable for the two incidents.

I have considered the mitigating conditions noted above, but the evidence is not sufficient to mitigate the concern. I reach that conclusion because the numerous incidents over a two-year period are evidence of a well-established pattern of negligence or lax security practices. The incidents are not so infrequent, few in number, or remote in time to assure me that similar incidents will not recur.

In addition to the formal mitigating conditions, I have considered the totality of the evidence, to include an examination of each security incident as developed during the hearing as well as an examination of the six incidents cumulatively. Consistent with Appeal Board caselaw, I have examined the six incidents in light of the very heavy burden of persuasion assigned to Applicant, and I have viewed his case in mitigation with strict scrutiny. I have considered the six security incidents in the context that Applicant has worked in the defense industry for about 18 years and has had a security clearance for most of that time. And I have considered that the six security incidents were inadvertent, resulting from simple oversight or an honest mistake. Applicant was well intentioned at all times.

In addition to the Guideline K matters, the SOR alleges the same six security incidents under Guideline E for personal conduct. The concern under Guideline E is decided against Applicant under the same rationale discussed above under Guideline K. The same judgment, trustworthiness, and reliability concerns present in Guideline E

are present in Guideline K. It is unnecessary to tread there further. The SOR also alleges the two incidents involving the AFT process under Guideline M for use of information technology. The concern under Guideline M is decided for Applicant because there has not been a final determination concerning Applicant's liability as well as the fact that others may have been held ultimately liable for the two incidents. Although these two incidents when taken together with the other four incidents are sufficient for adverse findings under Guidelines K and E, they are not sufficient for adverse findings under Guideline M when standing alone.

Following *Egan* and the clearly consistent standard, I have doubts or concerns about Applicant's reliability, trustworthiness, good judgment, and ability to protect classified or sensitive information. In reaching this conclusion, I weighed the evidence as a whole and considered if the favorable evidence outweighed the unfavorable evidence or *vice versa*. I also considered the whole-person concept. I conclude that he has not met his ultimate burden of persuasion to show that it is clearly consistent with the national interest to grant him eligibility for access to classified information.

Formal Findings

The formal findings on the SOR allegations are:

Paragraph 1, Guideline K:	Against Applicant
Subparagraphs 1.a – 1.f:	Against Applicant
Paragraph 2, Guideline M:	For Applicant
Subparagraph 2.a:	For Applicant
Paragraph 3, Guideline E:	Against Applicant
Subparagraph 3.a:	Against Applicant

Conclusion

It is not clearly consistent with the national interest to grant Applicant eligibility for access to classified information. Eligibility denied.

Michael H. Leonard
Administrative Judge