DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
----------	)	ISCR Case No. 17-01535
	)	
Applicant for Security Clearance	)	

Appearances

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

10/19/2018

_____

Decision

_____

LEONARD, Michael H., Administrative Judge:

Applicant contests the Defense Department's intent to revoke his eligibility for access to classified information. He explained the facts and circumstances surrounding a series of six security infractions occurring between April 2013 and March 2014. In addition, he has had no further security infractions or violations for the last four years. Taken together, the evidence is sufficient to mitigate the serious security concern stemming from the six infractions. Accordingly, this case is decided for Applicant.

Statement of the Case

Applicant completed and submitted a Standard Form (SF) 86, Questionnaire for National Security Positions, the official form used for personnel security investigations, on September 17, 2015.[1] This document is commonly known as a security clearance application. In addition, Applicant responded to a set of written interrogatories in June

[1] Exhibit 1.

2017.[2] Thereafter, on July 8, 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 detailed the factual reasons for the action under the security guideline known as Guideline K for handling protected information.

Applicant answered the SOR on July 26, 2017. He formally denied the allegations concerning six security infractions, but a review of his accompanying one-page memorandum shows that he admits receiving the infractions, but he denies that any classified information was disclosed or compromised, and he denies that any laboratory was left unsecured or unlocked. He also requested a hearing before an administrative judge.

The case was assigned to me on November 17, 2017. The hearing took place as scheduled on April 10, 2018. Applicant appeared without counsel. Department Counsel offered documentary exhibits, which were admitted as Exhibits 1-4. Other than Applicant, no witnesses were called by either party.

Procedural Matters

At hearing, the SOR was amended to change the date in ¶ 1.a from March 2012 to March 2014, which is in conformity with the evidence.[3]

Findings of Fact

Applicant is a 52-year-old product-test specialist who is seeking to retain a security clearance that he has held for decades. His first albeit brief marriage ended in divorce. He married for the second time in 2002. His formal education includes an associate's degree in applied science awarded in 1988. He has worked as a contracted-hourly employee for the same company (or its predecessor in interest) since 1993. Before that, beginning in about 1985, he worked as a student engineer for the same company (or its predecessor in interest). Altogether, he has about 30 years of service with his employer, and he is within a few years of retirement eligibility.[4]

As alleged in the SOR, Applicant committed and was disciplined for a series of six security infractions during the period of April 2013 through March 2014.[5] He endeavored to disclose the incidents when he completed his September 2015 SF 86, in which he stated that in March 2015 he had security violations, such as not signing the

[2] Exhibit 2.

[3] Tr. 12-14.

[4] Tr. 31-33.

[5] Exhibit 3.

log, and failure to flip a sign.[6] In addition to misstating the date in his SF 86, during his 2017 background investigation, he stated that he was not good with dates, and thought the incidents occurred between 2012 and 2015.[7] During the hearing, he repeatedly stated that he had not any further security incidents for the last two years, when in fact four years is correct.

The six incidents were determined to be infractions as opposed to violations, which are more serious. The first two infractions occurred in April and August 2013, while the last four occurred in March 2014 and involved a different laboratory than the 2013 incidents. The incidents involved the failure to properly secure a door or a closed area, or a failure to complete a security checklist. The six infractions were determined to be inadvertent. None involved compromise or disclosure of protected information or a mishandling of protected information. They were of a nature that there was little if any potential for disclosure of protected information.

Three of the March 2014 incidents occurred on three consecutive days (March 4, 5, and 6). Applicant was either not informed about his failure to properly secure the spin dial lock to secure a closed area, or he did not understand how to properly secure the spin dial lock, which resulted in repeated infractions of a similar nature. The door to the area itself was locked, but the spin dial lock was not properly secured.

Applicant received oral reprimands for the first two incidents in 2013. Concerning the four incidents in March 2014, it appears those matters were treated together for disciplinary purposes.[8] The relevant paperwork states he received two days off without pay, his open-and-close privileges were removed, and he no longer had certain combinations.[9] Applicant stated without equivocation that the two-day suspension was never implemented.[10]

Applicant attributed the six incidents to a combination of inadequate training or unclear instructions (e.g., he did not understand that he had to secure a spin dial lock by spinning it as opposed to setting it on zero, as was the practice with another laboratory), insufficient staffing (e.g., he was overwhelmed running two laboratories and attempted to turn down the assignment for the second), and lack of communication. He continues to have access to and has worked with protected information since his open-and-close privileges were removed in March 2014. He no longer works in the laboratory where he had the four incidents in March 2014.[11] He remains a designated employee who is

[6] Exhibit 1 at 9.

[7] Exhibit 2.

[8] Tr. 53-54; Exhibit 3 at 1-4.

[9] Exhibit 3 at 4.

[10] Tr. 69.

[11] Tr. 64-65.

responsible for securing all protected information in the event of an evacuation drill.[12] He receives recurrent security training from his employer. He has not been cited for any further security infractions or violations during the last four years.[13]

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.[14]

It is well-established law that no one has a right to a security clearance.[15] 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."[16] 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.[17] The Appeal Board has followed the Court's reasoning, and a judge's findings of fact are reviewed under the substantial-evidence standard.[18]

A favorable clearance decision establishes eligibility of an applicant to be granted a security clearance for access to confidential, secret, or top-secret information.[19] An unfavorable clearance decision (1) denies any application, (2) revokes any existing security clearance, and (3) prevents access to classified information at any level.[20]

[12] Tr. 27-28

[13] Tr. 65.

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

[15] *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).

[16] 484 U.S. at 531.

[17] 484 U.S. at 531.

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

[19] Directive, ¶ 3.2.

[20] Directive, ¶ 3.2.

There is no presumption in favor of granting, renewing, or continuing eligibility for access to classified information.[21] The Government has the burden of presenting evidence to establish facts alleged in the SOR that have been controverted.[22] An applicant is responsible for presenting evidence to refute, explain, extenuate, or mitigate facts that have been admitted or proven.[23] In addition, an applicant has the ultimate burden of persuasion to obtain a favorable clearance decision.[24]

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.[25]

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."[26] Put differently, security infractions and violations are serious business, and they are not to be taken lightly when evaluating an applicant's suitability.

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

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

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

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

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

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

[25] AG ¶ 33.

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

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;

AG ¶ 35(c) the security violations were due to improper or inadequate training or unclear instructions; 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 six security infractions within a short-term period during 2013-2014 establish a degree or pattern of negligence or laxness (or both) that is a very serious security concern. The above disqualifying conditions apply.

Concerning the mitigating conditions, Applicant receives credit under AG ¶ 35(a) based on the passage of time without recurrence of similar security infractions or violations. Recurrence is also unlikely because he was removed from open-and-close duty after the March 2014 incidents. Although he has had continued access to classified information to perform his job as a product-test specialist, he has now gone about four years without a further incident. And he remains a designated (and presumably trusted) employee who is responsible to secure protected information in the event of an evacuation drill.

AG ¶ 35(c) is also applicable because some of the infractions were due to inadequate training or unclear instructions. On that point, Applicant credibility explained during the hearing that he thought he was properly securing the spin dial lock used to secure a closed area when he committed three of the March 2014 incidents.

AG ¶ 35(d) is applicable too, in part. It applies to the extent that all six security infractions determined to be inadvertent, meaning they were unintentional, unintended, and not deliberate in nature. It also applies because there is no evidence of compromise or disclosure of protected information.

In addition to the formal mitigating conditions, I have considered the totality of the evidence, to include an examination of each security infraction as developed during the hearing as well as an examination of the six infractions cumulatively. Consistent with Appeal Board caselaw, I have examined the six infractions 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 also considered the six security infractions in the context that Applicant has worked in the defense industry for about 30 years and has had a security clearance for decades. In other words, the six security infractions during 2013-2014 amount to one very bad 12-month period during a long career working with protected

information. Having considered all these matters, I am satisfied that Applicant is an acceptable security risk within the meaning of our adjudicative process.[27]

Following *Egan* and the clearly-consistent standard, I have no 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 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:	For Applicant
Subparagraphs 1.a – 1.f:	For Applicant

Conclusion

It is clearly consistent with the national interest to grant Applicant access to classified information. Eligibility granted.

Michael H. Leonard
Administrative Judge

[27] AG ¶ 2(a).