DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
REDACTED	)	ISCR Case No. 17-01987
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Nicole A. Smith, Esq., Department Counsel
For Applicant: I. Charles McCullough III, Esq.

05/01/2018

_____

Decision

_____

MENDEZ, Francisco, Administrative Judge:

Applicant did not present sufficient evidence to mitigate security concerns raised by his deliberate security violation and egregious actions in undermining efforts to remediate a suspected spillage of classified information. Clearance is denied.

Statement of the Case

On June 30, 2017, the Department of Defense (DoD) sent Applicant a Statement of Reasons (SOR) alleging security concerns under Guideline K (handling protected information) and Guideline M (use of information technology). Applicant answered the SOR and requested a decision on the written record. Department Counsel requested a hearing in the matter, which was granted without objection. (Appellate Exhibit I).[1]

On April 17, 2018, a date mutually agreed to by the parties, a hearing was held. Applicant testified at the hearing and called his supervisor as a witness. Government Exhibits 1 and 2, as well as Applicant's Exhibits A – E, were admitted into the administrative record without objection. The transcript of the hearing was received on April 26, 2018.

[1] Department Counsel's discovery letter forwarding the exhibits that the Government planned on offering at the hearing was remarked post-hearing as Appellate Exhibit II.

Findings of Fact

Applicant, 46, is married with two children. He earned a mechanical engineering degree in 1995, and then enlisted in the U.S. military. He served in the military for 13 years, during which time he received his initial security clearance. He earned several advanced academic degrees while in the military and afterwards. He received an honorable discharge in 2008 and was then hired to work as a federal contractor by Company A. He is currently employed by Company B as a contractor supporting a federal law enforcement agency. He reports passing a counter-intelligence polygraph administered to him by the federal law enforcement agency and holding a top secret clearance with access to sensitive compartmented information (TS/SCI).[2]

In March 2015, Applicant was working for Company A. He was informed of a potential spillage of classified information and was directed by corporate security to turn in his company-issued cellphone. Applicant had received training on the proper procedures to follow in such situations and had experienced similar incidents in the past while working at Company A. In past incidents, company security would remotely wipe Applicant's company-issued cellphone. However, the company had recently changed from using blackberry devices to iPhones and corporate security requested that he turn in the iPhone. This was the first incident involving a suspected spillage with the new company-issued iPhone. Applicant did not turn in the iPhone. Instead, he turned in a different company cellphone. Sometime thereafter, Company A's security office confronted Applicant about the missing iPhone, which he then turned over. Applicant resigned in lieu of termination for violating security policies and procedures.[3]

Applicant explained his decision not to turn in his company iPhone and give security a different company cellphone as follows:

> I had many spinning plates in the air, and I just did not want to be inconvenienced . . . Looking back, I should have turned in the iPhone. But at the time, I just did not want to be inconvenienced and not have a -- been out of communication for a number of -- a few days, is what I expected.[4]

Applicant testified that at the time of the incident he did not have a personal cell phone and kept his personal contacts list on the company iPhone.[5] He previously told a security clearance investigator "that there was no personal information on the iPhone."[6]

Applicant did not talk to his supervisor about how to stay in touch with clients while corporate security completed its review of his company cellphone. He did not ask security

[2] Transcript (Tr.) 11-14, 20-21, 28; Exhibit 1; Exhibit A.

[3] Tr. 14-31; Exhibits 1, 2.

[4] Tr. 16, 24.

[5] Tr. 29-30.

[6] Exhibit 2 at 3.

how long it would take them to review and sanitize the cellphone.[7] However, he "was aware that he would eventually be provided with the iPhone back, or with an alternate work phone, but he did not want to wait for that to happen."[8]

Applicant testified that after not turning in the iPhone, he realized his mistake and planned to turn it in the next morning. But, he was contacted by corporate security before he could voluntarily turn in the phone.[9] Applicant explained the security incident leading to his resignation from Company A in his security clearance application, which he certified as true and accurate on March 19, 2016, as follows:

> [Company A] security office initiated the steps to address the data spill and requested that I surrender the cell phone. I did not surrender the phone as requested. The security office was able to determine that I still had the phone in my possession. *Eventually*, the security office personnel produced evidence that I had my cell phone at which time I surrendered the phone as directed. As a consequence of my misconduct and violation of [Company A] security policies, I resigned in lieu of termination from [Company A].[10]

Applicant states that he has changed his security posture since the 2015 incident, noting he will "not accept a government cell phone."[11] He further states that since the incident he has complied with all security rules and regulations, including complying with all direction for safeguarding information and systems following a suspected spillage.[12]

Applicant is well regarded by his employer and others for his professionalism, reliability, and trustworthiness.[13] Applicant testified that he told his program manager, a special supervisory agent (SSA) with the federal law enforcement agency for which Applicant now works as a contractor, about the 2015 security incident. On direct examination, Applicant testified as follows about his purported conversations with the SSA about the incident:

> Question: Now, does [federal law enforcement agency] know about this whole situation?
>
> Applicant: Yes, the [agency] does know about the situation.
>
> Question: How do you know the [agency] knows about this situation?

[7] Tr. 28-31.

[8] Exhibit 2 at 3.

[9] Tr. 17-18.

[10] Exhibit 1 at 16-17 (emphasis added).

[11] Tr. 25.

[12] Tr. 19-20, 25.

[13] Tr. 33-40; Exhibits D, E.

> Applicant: At the time, I was working with Supervisory Special Agent [X]. I told [him] what happened, number one.[14]

The SSA testified at the hearing and stated that he was "somewhat" aware of the incident.[15] The SSA went on to state that he was "back briefed" on the incident by his security manager, and "was given enough to know or visibility on what might be a potential issue."[16] The SSA further explained his understanding of the 2015 security incident:

> Well, again, this was, again, discussions between my security officer and the others, so it's almost I wasn't part of the conversations. Information had been from -- I guess a spill, as a lack of a better term -- to an unclassified medium and that there was a process to address that. And that that process -- I guess there were some issues there, potential issues, based on others' opinions and analysis about the limit of my visibility on it.[17]

The SSA did not testify about a direct conversation with Applicant about the incident.

Law, Policies, and Regulations

This case is decided under Executive Order (E.O.) 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 National Security Adjudicative Guidelines (AG), which became effective on June 8, 2017.

"[N]o one has a 'right' to a security clearance." *Department of the Navy v. Egan*, 484 U.S. 518, 528 (1988). Instead, persons are only eligible for access to classified information "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. 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. AG ¶ 2.

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

[14] Tr. 18-19.

[15] Tr. 37; Exhibits B, C.

[16] Tr. 39.

[17] Tr. 39-40.

proven . . . and has the ultimate burden of persuasion as to obtaining a favorable clearance decision." Directive ¶ E3.1.15.

Administrative Judges must remain fair and impartial, and carefully balance the needs for the expedient resolution of a case with the demands of due process. Therefore, an administrative judge will ensure that an applicant: (a) receives fair notice of the issues, (b) has a reasonable opportunity to address those issues, and (c) is not subjected to unfair surprise. Directive, ¶ E3.1.10; ISCR Case No. 12-01266 at 3 (App. Bd. Apr. 4, 2014).

In evaluating the evidence, a judge applies a "substantial evidence" standard, which is something less than a preponderance of the evidence. Specifically, substantial evidence is defined as "such relevant evidence as a reasonable mind might accept as adequate to support a conclusion in light of all the contrary evidence in the same record." Directive, ¶ E3.1.32.1.[18]

Any doubt raised by the evidence must be resolved in favor of the national security. AG ¶ 2(b). *See also* Security Executive Agent Directive 4 (SEAD 4), ¶ E.4. Additionally, the Supreme Court has held that responsible officials making "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 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 ¶ 33)

In assessing Applicant's case, I considered the applicable disqualifying and mitigating conditions, including:

[18] However, a judge's mere disbelief of an applicant's testimony or statements, without actual evidence of disqualifying conduct or admission by an applicant to the disqualifying conduct, is not enough to sustain an unfavorable finding. ISCR Case No. 15-05565 (App. Bd. Aug. 2, 2017); ISCR Case No. 02-24452 (App. Bd. Aug. 4, 2004). Furthermore, an unfavorable decision cannot be based on non-alleged conduct. ISCR Case No. 14-05986 (App. Bd. May 26, 2017). Unless an applicant is provided notice that unalleged conduct raises a security concern, it can only be used for specific limited purposes, such as assessing mitigation and credibility. ISCR Case No. 16-02877 at 3 (App. Bd. Oct. 2, 2017).

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

AG ¶ 35(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; 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.

In most cases administrative judges are called upon to make predictive judgments about a person's security clearance suitability based on conduct or circumstances that are unrelated to the actual mishandling of protected information. When a person, however, previously mishandled protected information or violated a security rule or regulation, such a person bears a heavy burden in reestablishing their eligibility for a security clearance.[19] Here, Applicant failed to meet his burden of proof and persuasion.

Applicant's security violation and actions in delaying and undermining his former employer's efforts to remediate a suspected spillage of protected information was knowing, deliberate, and egregious. AG ¶ 34(g) applies. Although the incident occurred a little over three years ago, insufficient time has passed to safely conclude that Applicant has reformed his past behavior and a similar security-significant incident will not recur. In reaching this conclusion, I have considered Applicant's expression of remorse, overall security record, and his work performance, both before and since the incident. However, this and the other favorable record evidence are insufficient to mitigate the heightened security concerns raised by the egregious and deliberate nature of the security violation at issue. Furthermore, Applicant's testimony appears at odds with his past statements during the security clearance process about the incident and his witnesses' testimony. AG ¶¶ 35(a) and 35(b) do not apply.

Guideline M, 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. (AG ¶ 39)

[19] ISCR Case No. 11-10255 at 5 (App. Bd. July 28, 2014) ("Once it is established that an applicant has committed a security violation, he or she has a 'very heavy burden' of persuasion that he or she should have a clearance. [Because,] [s]ecurity violations 'strike at the heart of the industrial security program.'") citing, ISCR Case No. 10-04911 at 5 (App. Bd. Dec. 19, 2011).

Applicant's misconduct also raises similar security concern under Guideline M and for similar reasons noted above the evidence he presented was insufficient to mitigate those concerns. AG ¶¶ 40(b) and 40(e) apply.[20] None of the mitigating conditions apply.

Whole-Person Concept

In addition to the specific adjudicative guidelines, a judge must also consider the non-exclusive group of factors falling under the whole-person concept.[21] I hereby incorporate my above analysis and highlight some additional whole-person matters.

Applicant served in the military for 13 years and thereafter has worked as a federal contractor. His security record was spotless before and after the 2015 incident. Additionally, after the incident, Applicant was vetted by a federal law enforcement agency. However, the deliberate and egregious nature of the security violation at issue, coupled with Applicant's less-than-candid statements during the security clearance process, raise heightened security concerns that continue to raise serious questions and doubts about his suitability for continued access to classified information.[22]

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:	AGAINST APPLICANT
Subparagraph 1.a:	Against Applicant
Paragraph 2, Guideline M:	AGAINST APPLICANT
Subparagraph 2.a:	Against Applicant

Conclusion

In light of the record evidence, it is not clearly consistent with the interests of national security to grant Applicant initial or continued eligibility for access to classified information. Applicant's request for a security clearance is denied.

Francisco Mendez
Administrative Judge

[20] AG ¶ 40(b) (". . . denial of access to an information technology system or any data in such a system); AG ¶40(e) ("unauthorized use of any information technology system.").

[21] *See* AG ¶ 2. *See also* SEAD-4, ¶ E.4; Directive, ¶ 6.3.

[22] I also considered the exceptions listed in SEAD 4, Appendix C, especially in light of Applicant's counsel's closing argument pointing out Applicant's unique skills and contributions to the national defense. However, Applicant did not provide sufficient evidence to warrant application of any of the exceptions in Appendix C.