DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 18-02968
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Kelly Folks, Esq., Department Counsel
For Applicant: Kel McClanahan, Esq.

10/10/2019

_____

Decision

_____

Curry, Marc E., Administrative Judge:

Although Applicant's removal of a classified disk from her office was inadvertent, she did not disclose it to her employer until 18 months later, before a scheduled polygraph examination. Under these circumstances, she has failed to mitigate the security concern. Clearance is denied.

Statement of the Case

On February 21, 2019, the Department of Defense Consolidated Adjudications Facility (DOD CAF) issued a Statement of Reasons (SOR) to Applicant, detailing the security concern under Guideline K, handling protected information, explaining why it was unable to find it clearly consistent with the national security to grant security clearance eligibility. The DOD CAF took the action under Executive Order (EO) 10865, *Safeguarding Classified Information within Industry* (February 20, 1960), as amended; and DOD Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (January 2, 1992), as amended (Directive) and the National Security Adjudicative Guidelines (AG), effective June 8, 2017.

On March 11, 2019, Applicant answered the SOR, admitting in part the allegation

and denying it in part. She requested a hearing, whereupon the case was assigned to me on May 7, 2019. On July 17, 2019, DOHA scheduled the case for August 8, 2019. At the hearing, I received three Government Exhibits, marked and admitted as GE 1 through GE 3, one Applicant exhibit (AE A), and Applicant's testimony. Also, I incorporated a copy of Department Counsel's discovery letter to Applicant, dated April 11, 2019, into the record. (Hearing Exhibit I) At Applicant's request, I left the record open to enable her to submit additional exhibits. Within the time allotted, her counsel submitted an additional exhibit, marked and admitted as AE B. The transcript (Tr.) was received on August 30, 2019

Findings of Fact

Applicant is a 44-year-old married woman. She graduated from college in 1997 and earned a master's degree in 2007. (Tr. 49) She has worked for various federal contractors since 2006. She currently is a data scientist. (Tr. 32) She has held a security clearance since 2006. (Tr. 55)

Applicant is highly respected on the job. According to her supervisor, she is unique because she understands all of the technology that her company utilizes at an expert level. (Tr. 70) Moreover, she is highly security conscious, as she is typically the employee who asks if everyone has the necessary clearances before engaging in conversations with clients. (Tr. 71)

In March 2015, towards the end of a contract, Applicant and her coworkers were instructed to clean out their work areas, pack their belongings and telework until the next project started. Applicant complied with this directive, packing her personal belongings in a box and taking them home. (Tr. 37)

About three weeks later, in April 2015, Applicant realized that she had inadvertently taken a classified CD home. (Tr. 37, 63) She immediately rendered it inoperable by scratching it and breaking it into several pieces. (Tr. 36). She stored the broken, inoperable CD in a box in her garage until approximately September 2015, after her employer regained access to the sensitive compartmented information facility. (Tr. 65) She then returned it to the SCIF, but did not inform the facility security office that she had removed it. Her failure to report the return of the classified pieces of the CD stemmed from a combination of fear, procrastination, and the prioritization of project work over security consciousness. (GE B at 3; Tr. 37) Specifically, when she initially returned the CD, she did not want to take the time to report it to the facility security officer because the process was time-consuming, and she preferred to spend her time completing a project. (Tr. 38) She ultimately disclosed the information about the CD during a polygraph examination in September 2016. (Tr. 38)

Policies

The U.S. Supreme Court has recognized the substantial discretion the Executive Branch has in regulating access to information pertaining to national security, emphasizing that "no one has a 'right' to a security clearance." *Department of the Navy v. Egan*, 484

U.S. 518, 528 (1988). 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 listpotentially disqualifying conditions and mitigating conditions, which are required to be considered 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 together with the factors listed in the adjudicative process. The administrative judge's overall adjudicative goal is a fair, impartial, and commonsense decision. According to AG ¶ 2(c), the entire process is a conscientious scrutiny 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, the applicant is responsible for presenting "witnesses and other evidence to rebut, explain, extenuate, or mitigate facts admitted by applicant or proven by Department Counsel. . . ." The applicant 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 the 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 Executive Order 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).

Under the whole-person concept, the administrative judge must consider the totality of an applicant's conduct and all relevant circumstances in light of the nine adjudicative process factors in AG ¶ 2(d). They are as follows:

(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.

Analysis

Guideline K: Handling Protected Information

The security concerns about handing protected information are set forth in AG ¶ 13:

> 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.

Applicant's conduct with respect to the classified CD that she took home in 2015 triggers the application of AG ¶ 34(b), "collecting or storing protected information in any unauthorized location, and AG ¶ 34(g), "any failure to comply with rules for the protection of classified or sensitive information." Applicant's removal of the CD from her office was inadvertent and happened under an unusual circumstance, as she was moving out of her office during the pending expiration of a contract. Conversely, although she destroyed the CD, she did not report the removal until she was scheduled to take a polygraph, approximately 18 months after she had removed it from the SCIF. This renders the mitigating condition in AG ¶ 35(d), "the violation was inadvertent, it was promptly reported, there is no evidence of compromise, and it does not suggest a pattern," inapplicable.

Although the nature of the circumstances surrounding the inadvertent removal of the CD from the SCIF was unusual, it has no bearing on Applicant's conscious decision not to immediately report the violation. Moreover, given the nature and seriousness of Applicant's security violation, not enough time has elapsed since the conduct to conclude that it is mitigated by the passage of time. I conclude 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," does not apply.

Applicant received annual security briefings before she committed the security violation. She understood when she discovered that she had accidentally brought the CD home, and later, when she returned it, but failed to surrender it to the FSO's office, that her actions were inconsistent with the lessons taught in the annual security briefings. AG ¶ 35(c), "the security violations were due to improper or inadequate training or unclear instructions," does not apply. Nevertheless, Applicant is contrite and understands that she must not subordinate her security responsibilities to her work responsibilities. She has continued to attend annual security briefings from her employer. 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," applies.

Whole-Person Concept

Given the nature and seriousness of Applicant's failure to report her security violation for more than a year after it occurred, it is too soon to conclude that such conduct may not recur. In reaching this conclusion, I was cognizant of DOHA jurisprudence which treats security violations with particular gravity, and which establishes a strict scrutiny standard for evaluating mitigation.

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

Conclusion

In light of all of the circumstances presented by the record in this case, it is not clearly consistent with the interests of national security to grant Applicant eligibility for a security clearance. Eligibility for access to classified information is denied.

_____
Marc E. Curry
Administrative Judge