



**DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS**



In the matter of:)	
)	
[Redacted])	ISCR Case No. 14-06907
)	
Applicant for Security Clearance)	

Appearances

For Government: Carroll J. Connelly, Esq., Department Counsel
For Applicant: *Pro se*

10/31/2016

Decision

FOREMAN, LeRoy F., Administrative Judge:

This case involves security concerns raised under Guideline K (Handling Protected Information). Eligibility for access to classified information is granted.

Statement of the Case

Applicant submitted a security clearance application (SCA) on February 19, 2014, seeking to continue her security clearance. On August 25, 2015, the Department of Defense (DOD) sent her a Statement of Reasons (SOR), alleging security concerns under Guideline K. The DOD acted under Executive Order (Exec. Or.) 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 DOD on September 1, 2006. The AG are codified in 32 C.F.R. § 154, Appendix H (2006), and they replace the guidelines in Enclosure 2 to the Directive.

Applicant answered the SOR on November 25, 2015, and requested a decision on the record without a hearing. Department Counsel submitted the Government's

written case on February 1, 2016. On February 4, 2016, a complete copy of the file of relevant material (FORM) was sent to Applicant, who was given an opportunity to file objections and submit material to refute, extenuate, or mitigate the Government's evidence. The FORM included the SOR and her answer (Item 1), her SCA (Item 2), a summary of a personal subject interview (PSI) by a security investigator in May 2014 (Item 3), and a Joint Personnel Adjudication System (JPAS) incident report (Item 4.) She received the FORM on February 16, 2016, and she timely submitted a statement, which was admitted without objection and included in the record as Applicant's Exhibit (AX) A. The case was assigned to me on October 19, 2016.

Evidentiary Issue

Item 3, the May 2014 PSI, was not authenticated as required by Directive ¶ E3.1.20. However, Applicant was informed by Department Counsel that she was entitled to make corrections, additions, deletions, and updates to Item 3. She was also informed that she was entitled to object to consideration of Item 3 on the ground that it was not authenticated. Her failure to comment on the accuracy of Item 3 or object to it constitutes a waiver of any objection to it. See ISCR Case No. 12-10810 at 2 (App. Bd. Jul. 12, 2016) ("Although *pro se* applicants are not expected to act like lawyers, they are expected to take timely and reasonable steps to protect their rights under the Directive.")

Findings of Fact¹

In her answer to the SOR, Applicant admitted the allegations in SOR ¶¶ 1.b-1.e. She neither admitted nor denied the allegation in SOR ¶ 1.a, stating that she could not remember the incident. Her admissions in her answer are incorporated in my findings of fact.

Applicant is a 58-year-old industrial security specialist employed by a defense contractor since August 1979. She attended college from September 1976 to December 1978 but did not receive a degree. She has never married and has no children. She has held a security clearance since October 1979. (Item 3 at 4.)

Applicant's duties included opening and closing sensitive compartmented information facilities (SCIFs). In November 2012, Applicant locked all the classified safes in her work area toward the end of the work day. As she was preparing to leave for the day, she reopened a safe at the request of an employee and forgot to relock it. In March 2013 and April 2013, she left a safe unlocked under similar circumstances, reopening it at the end of the work day and neglecting to relock it. In each case, she attributed her dereliction to fatigue and being rushed. The safes were in a secure area, no intrusion alarms were triggered, and the unlocked safes were discovered by coworkers. In each instance, an investigation determined that no classified information was compromised. The procedures for securing classified safes were changed after the

¹ Applicant's personal information is extracted from her security clearance application (Item 2) unless otherwise indicated by a parenthetical citation to the record.

April 2013 incident, and the current procedures provide for locking the safes 15 minutes before the end of the work day and not unlocking them until the following work day. (Item 3 at 2-3.)

In January 2013, Applicant sent an email containing personal information by unclassified email to another industrial security specialist employed by the same defense contractor. The email was encrypted, but sending it by email outside her department violated her employer's rules for handling personal information. The recipient of the email reported the incident. Applicant attributed this dereliction to being rushed and failing to check the email for personal information before sending it. She told a security investigator that the incident occurred at a time when her employer was deciding how to handle personal information and that the procedures were often changed. (Item 3 at 2-3.) The record does not reflect what procedures were in effect and were violated by Applicant's actions. However, Applicant admitted that she knew she had inadvertently violated the procedures that were then in effect.

After the April 2013 incident, Applicant received a corrective action memo (CAM) and was suspended for one day without pay. In a personal subject interview (PSI) conducted in May 2014, Applicant stated that she received a CAM for each incident, but the record reflects that the April 2013 CAM covered all four incidents. (Item 3 at 2; Item 4.)

Applicant's derelictions occurred at a time when she was dealing with grief following the deaths of her parents, the death of an aunt after a long battle with cancer, and the memory loss suffered by her uncle (her deceased aunt's husband). Since October 2013, she has lived with her uncle and cared for him. (Item 2 at 7.) She received grief counseling from a licensed clinical social worker and believes that she has returned to her "normal triple-checking obsessive self." (AX A.)

Policies

"[N]o one has a 'right' to a security clearance." *Department of the Navy v. Egan*, 484 U.S. 518, 528 (1988). As Commander in Chief, the President has the authority to "control access to information bearing on national security and to determine whether an individual is sufficiently trustworthy to have access to such information." *Id.* at 527. The President has authorized the Secretary of Defense or his designee to grant applicants eligibility for access to classified information "only upon a finding that it is clearly consistent with the national interest to do so." Exec. Or. 10865 § 2.

Eligibility for a security clearance is predicated upon the applicant meeting the criteria contained in the AG. These guidelines are not inflexible rules of law. Instead, recognizing the complexities of human behavior, an administrative judge applies these guidelines in conjunction with an evaluation of the whole person. An administrative judge's overarching adjudicative goal is a fair, impartial, and commonsense decision. An administrative judge must consider all available and reliable information about the person, past and present, favorable and unfavorable.

The Government reposes a high degree of trust and confidence in persons with access to classified information. This relationship transcends normal duty hours and endures throughout off-duty hours. 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.

Clearance decisions must be made “in terms of the national interest and shall in no sense be a determination as to the loyalty of the applicant concerned.” Exec. Or. 10865 § 7. Thus, a decision to deny a security clearance is merely an indication the applicant has not met the strict guidelines the President and the Secretary of Defense have established for issuing a clearance.

Initially, the Government must establish, by substantial evidence, conditions in the personal or professional history of the applicant that may disqualify the applicant from being eligible for access to classified information. The Government has the burden of establishing controverted facts alleged in the SOR. See *Egan*, 484 U.S. at 531. “Substantial evidence” is “more than a scintilla but less than a preponderance.” See *v. Washington Metro. Area Transit Auth.*, 36 F.3d 375, 380 (4th Cir. 1994). The guidelines presume a nexus or rational connection between proven conduct under any of the criteria listed therein and an applicant’s security suitability. See ISCR Case No. 92-1106 at 3, 1993 WL 545051 at *3 (App. Bd. Oct. 7, 1993).

Once the Government establishes a disqualifying condition by substantial evidence, the burden shifts to the applicant to rebut, explain, extenuate, or mitigate the facts. Directive ¶ E3.1.15. An applicant has the burden of proving a mitigating condition, and the burden of disproving it never shifts to the Government. See ISCR Case No. 02-31154 at 5 (App. Bd. Sep. 22, 2005).

An applicant “has the ultimate burden of demonstrating that it is clearly consistent with the national interest to grant or continue his security clearance.” ISCR Case No. 01-20700 at 3 (App. Bd. Dec. 19, 2002). “[S]ecurity clearance determinations should err, if they must, on the side of denials.” *Egan*, 484 U.S. at 531; see AG ¶ 2(b).

Analysis

Guideline K, Handling Protected Information

The SOR alleges that Applicant failed to properly transmit classified material in June 2011 (SOR ¶ 1.a), failed to properly secure a safe in November 2012, March, 2013, and April 2013 (SOR ¶¶ 1.b, 1.e, and 1.e), and improperly sent “privacy information” through regular email in January 2013 (SOR ¶ 1.c). AG ¶ 33 expresses the security concern pertaining to 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.”

Security violations are one of the strongest possible reasons for denying or revoking access to classified information, as they raise very serious questions about an applicant's suitability for access to classified information. Once it is established that an applicant has committed a security violation, he or she has a very heavy burden of demonstrating that he or she should be entrusted with classified information. Because security violations strike at the very heart of the industrial security program, an administrative judge must give any claims of reform and rehabilitation strict scrutiny. See ISCR Case No. 03-26888 (App. Bd. Oct. 5, 2006). The frequency and duration of the security violations are aggravating factors. ISCR Case No. 97-0435 at 5 (App. Bd. July 14, 1998).

There is no evidence in the record supporting the allegation in SOR ¶ 1.a. However, the evidence in the FORM and Applicant's admissions established the allegations in SOR ¶¶ 1.b-1.e, and they are sufficient to establish the disqualifying condition in AG ¶ 34(g) (“any failure to comply with rules for the protection of classified or other sensitive information”). AG ¶ 34(h) (“negligence or lax security habits that persist despite counseling by management”) is not established, because there is no evidence that Applicant was counseled until after her last violation, and there is no evidence of any violations after she received the CAM.

The following mitigating conditions are potentially applicable:

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.

Both mitigating conditions are established. Applicant had multiple violations within a five-month period, and they did not occur under unusual circumstances. However, three and a half years have passed since her last violation. She responded positively to the corrective action. She obtained counseling to help her deal with her grief. Her uncle's situation has stabilized. Her employer has adopted procedures to prevent the stressful and risky practice of reopening and relocking classified safes at the last minute before the end of the work day. Under these circumstances, Applicant's derelictions are unlikely to recur, and they do not cast doubt on her current reliability, trustworthiness, or good judgment.

Whole-Person Concept

Under AG ¶ 2(c), the ultimate determination of whether to grant eligibility for a security clearance must be an overall commonsense judgment based upon careful consideration of the guidelines and the whole-person concept. In applying the whole-person concept, an administrative judge must evaluate an applicant's eligibility for a security clearance by considering the totality of the applicant's conduct and all relevant circumstances. An administrative judge should consider the nine adjudicative process factors listed at AG ¶ 2(a):

(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.

I have incorporated my comments under Guideline K in my whole-person analysis. Some of the factors in AG ¶ 2(a) were addressed under that guideline, but some warrant additional comment.

Because Applicant requested a determination on the record without a hearing, I have no opportunity to evaluate her credibility and sincerity based on demeanor. See ISCR Case No. 01-12350 at 3-4 (App. Bd. Jul. 23, 2003). However, the record reflects that she has worked for the same employer and held a security clearance for more than 37 years. She understands that her violations were serious. She has expressed remorse and taken positive steps to set her personal life in order.

After weighing the disqualifying and mitigating conditions under Guideline K, and evaluating all the evidence in the context of the whole person, I conclude Applicant has mitigated the security concerns raised by her derelictions in handling classified and sensitive information. Accordingly, I conclude she has carried her burden of showing that it is clearly consistent with the national interest to continue her eligibility for access to classified information.²

² Administrative judges do not have authority to grant conditional clearances. ISCR Case No. 99-0901, 2000 WL 288429 at *3 (App. Bd. Mar.1, 2000). However, any future failure to comply with rules for the protection of classified or other sensitive information may well trigger a reconsideration of Applicant's eligibility for access to classified information. See ISCR Case No. 10-06943 at 4 (App. Bd. Feb. 17, 2012).

Formal Findings

I make the following formal findings on the allegations in the SOR:

Paragraph 1, Guideline K (Handling Protected Information): FOR APPLICANT

Subparagraphs 1.a-1.e:

For Applicant

Conclusion

I conclude that it is clearly consistent with the national interest to continue Applicant's eligibility for a security clearance. Eligibility for access to classified information is granted.

LeRoy F. Foreman
Administrative Judge