DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 18-01500
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Mary M. Foreman, Esq., Department Counsel
For Applicant: Charles Bell, Personal Representative

02/06/2019

_____

Decision

_____

CERVI, Gregg A., 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 June 14, 2016. On June 15, 2018, the Department of Defense Consolidated Adjudications Facility (DOD CAF) sent her a statement of reasons (SOR) alleging security concerns under Guideline K.[1] Applicant answered the SOR and requested a hearing.

The case was assigned to me on August 20, 2018. The Defense Office of Hearings and Appeals (DOHA) issued a notice of hearing on August 20, 2018, scheduling the hearing for August 27, 2018. The hearing was convened as scheduled. Government

[1] The DOD CAF acted under Executive Order (Exec. Or.) 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). The Adjudicative Guidelines (AG) were revised effective June 8, 2017, and apply herein.

Exhibits (GE) 1 through 3 were admitted in evidence without objection. Applicant and three witnesses testified, and Applicant Exhibit (AE) A was admitted without objection. DOHA received the hearing transcript (Tr.) on September 6, 2018.

Findings of Fact

Applicant is a 34-year-old personnel security representative for a defense contractor, employed since 2008. She was awarded a bachelor's degree in 2006 and a master's degree in 2012. She is married and has no children. She has held a security clearance since 2008.

The SOR alleges Applicant had four security infractions from 2008 to 2017. She admitted the allegations, with explanations. In 2008, while new to the company, Applicant inadvertently carried a camera in her handbag into a closed area where she worked. She sat at her desk, and was looking through her handbag when she discovered the camera. At the time, cameras, but not cell phones, were prohibited in the space. The camera remained off, and Applicant immediately showed the camera to her security manager. The company reported that no classified information was put at risk in the incident.

In 2015, Applicant inadvertently scanned two program access requests (PAR) into a computer system. The PAR is unclassified but contains sensitive personal information. Applicant and another employee, both new to the position, were tasked to scan thousands of PARs as a group, into a computer system. The employees were not required to review each document for sensitive information, but a random check was done. After the PARs were entered into the computer system, Applicant noticed two PARs with sensitive information that should not have been scanned, and reported it to her security manager. Applicant's supervisor, the company's security manager, testified that the incident was not Applicant's fault, rather, she completed the task as directed and could not have known the two particular PARs in the stack of PARs held sensitive information. The incident was reported and investigated as an infraction so that it could be properly documented, but no loss or compromise of sensitive information was found.

In 2016, Applicant was again tasked to scan documents into a computer system, but to redact with a black marker, sensitive, unclassified data on some documents before scanning them. According to Applicant's security manager, Applicant followed directions exactly as tasked, but noticed that some redacted documents still showed information through the redaction after scanning. Again, the security manager testified that Applicant was not at fault for the incident, but that she followed directions exactly as tasked, and Applicant reported the incident as soon as it was discovered. The company's method of redaction was changed. Again, the incident was reported and investigated as an infraction so that it could be properly documented, but no loss or compromise of sensitive information was found.

In 2017, Applicant allowed an unauthorized individual into a classified space. Applicant was tasked to provide a classified security briefing to new employees. She was provided a classified cover sheet from the government client, listing employees to be

briefed. The cover sheet identified all listed employees as cleared, but the underlying PAR for one of the employees was "disapproved" and should not have appeared on the cover sheet. Applicant reviewed the cover sheet, but did not realize that one employee listed was disapproved on his PAR. Applicant conducted the brief, but afterward she found that the cover sheet misidentified the employee as approved for the brief and reported the incident to her supervisor. The employee was eventually approved for the brief. The incident was referred to the on-site Air Force Office of Special Investigations (OSI) agent, who testified on behalf of Applicant. The OSI agent indicated that the government client misidentified the employee, and that the improper briefing was not the fault of Applicant. He has worked with Applicant on a regular basis and believes she is honest and trustworthy. He unequivocally recommends Applicant retain her security clearance.

Applicant acknowledged the security incidents and took responsibility for all of the incidents, despite the fact that three of the four incidents were outside of her responsibility. The company compliance lead, Applicant's current security manager, and on-site OSI agent testified on behalf of Applicant and attested that she was not directly responsible for the last three incidents and the camera incident was minor. They all believe that Applicant's honesty and trustworthiness make her a unique fit for the security office and that she complies with security rules and regulations. Applicant promptly reported all infractions once discovered and learned how to prevent further incidents in the future.

Law and 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.

National security eligibility is predicated upon the applicant meeting the criteria contained in the adjudicative guidelines. 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 a person's stability, trustworthiness, reliability, discretion, character, honesty, and judgment. AG ¶ 1(b).

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. *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, e.g.,* ISCR Case No. 12-01295 at 3 (App. Bd. Jan. 20, 2015).

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, e.g.,* 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 ¶ 1(d).

Analysis

Guideline K: Handling Protected Information

AG ¶ 33 expresses the handling protected information security concern:

> 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.

Relevant conditions that could raise a security concern under AG ¶ 34 and may be disqualifying include:

> (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; and

(g) any failure to comply with rules for the protection of classified or sensitive information.

Applicant's involvement in the security incidents alleged in the SOR are generally insufficient to directly implicate disqualifying security concerns under AG ¶ 34. However, even if Applicant's record of involvement or relationship with security infractions raises concerns under AG ¶ 34, they are clearly mitigated under AG ¶ 35.

Relevant conditions that could mitigate security concerns under AG ¶ 35 include:

(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;

(b) the individual responded favorably to counseling or remedial security training and now demonstrates a positive attitude toward the discharge of security responsibilities;

(c) the security violations were due to improper or inadequate training or unclear instructions; and

(d) the violation was inadvertent, it was promptly reported, there is no evidence of compromise, and it does not suggest a pattern.

Except for a minor infraction in 2008 when Applicant inadvertently took an unused camera in her handbag into a closed facility, the more significant infractions were not caused by Applicant's intentional actions or negligence. Applicant performed her duties as directed, but the direction and training were insufficient to prevent the security incidents from occurring. Applicant self-reported all of the incidents, learned to prevent them in the future, and is more attune to the potential pitfalls during similar tasks. Her compliance lead, security manager, and on-site OSI agent who works closely with Applicant strongly support her and attest to her trustworthiness and honesty. AG ¶¶ 35 (a), (b), (c), and (d) apply.

Whole-Person Concept

Under AG ¶¶ 2(a), 2(c), and 2(d), the ultimate determination of whether to grant national security eligibility must be an overall commonsense judgment based upon careful consideration of the guidelines and the whole-person concept. Under the whole-person concept, the 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. The administrative judge should consider the nine adjudicative process factors listed at AG ¶ 2(d). Although adverse information concerning a single criterion may not be sufficient for an unfavorable eligibility determination, the individual may be

found ineligible if available information reflects a recent or recurring pattern of questionable judgment, irresponsibility, or unstable behavior. AG ¶ 2(e).

I considered all of the potentially disqualifying and mitigating conditions in light of the facts and circumstances surrounding this case. I have incorporated my findings of fact and comments under Guideline K in my whole-person analysis. Applicant is a mature employee with many years of handling classified information in sensitive spaces, and she is trusted and honest. She has acknowledged the security lapses that led to the incidents in question, and understands how to prevent such occurrences going forward. The favorable record evidence is sufficient to fully mitigate the security concerns raised in the SOR.

Overall, the record evidence leaves me without questions or doubts as to Applicant's eligibility for continued access to classified information. Accordingly, I conclude Applicant has carried her burden of showing that it is clearly consistent with the national security interests of the United States to continue his eligibility for access to classified information.

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:	FOR APPLICANT
Subparagraphs 1.a – 1.d:	For Applicant

Conclusion

I conclude that it is clearly consistent with the national security to grant continued eligibility for access to classified information. Applicant's request for security eligibility is granted.

_____
Gregg A. Cervi
Administrative Judge