



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



In the matter of:	)	
	)	
	)	ISCR Case No. 14-03659
	)	
Applicant for Security Clearance	)	

**Appearances**

For Government: Allison O'Connell, Esq., Department Counsel  
For Applicant: James Y. Boland, Esq.

11/20/2015

**Decision**

RIVERA, Juan J., Administrative Judge:

Applicant's security violations demonstrated negligence and lack of judgment. She expressed remorse and took responsibility for her actions. She has demonstrated a renewed, positive attitude toward the discharge of her security responsibilities. Considering her performance, credible contrition, and her current attitude toward the discharge of her security responsibilities, I find Applicant's past security violations are unlikely to recur and do not cast doubt on her current reliability, trustworthiness, and judgment. Clearance granted.

**Statement of the Case**

Applicant submitted her most recent security clearance application (SCA) on August 23, 2011. On April 4, 2015, the Department of Defense (DOD) issued Applicant a Statement of Reasons (SOR) listing security concerns under Guideline K (handling protected information).<sup>1</sup>

---

<sup>1</sup> DOD acted under Executive Order 10865, *Safeguarding Classified Information Within Industry* (February 20, 1960), as amended; DOD Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (Directive) (January 2, 1992), as amended; and the *Adjudicative Guidelines*

Applicant answered the SOR on April 29, 2015, and requested a hearing before an administrative judge. The case was assigned to me on July 30, 2015. The Defense Office of Hearings and Appeals (DOHA) issued the hearing notice on July 31, 2015, convening a hearing for August 27, 2015. At the hearing, the Government offered exhibits (GE) 1 through 8. Applicant testified and submitted one exhibit (AE 1). All exhibits were admitted without objection. DOHA received the hearing transcript (Tr.) on September 10, 2015.

### **Findings of Fact**

In her answer to the SOR (Answer), Applicant admitted the factual allegations in SOR ¶¶ 1.a and 1.b, with comments. She failed to admit or deny the allegation in SOR ¶ 1.c. I considered the allegation denied. Applicant's admissions are incorporated herein as findings of fact. After a thorough review of all the evidence, including her testimony and demeanor while testifying, I make the following additional findings of fact:

Applicant is a 56-year-old facility security officer (FSO) working for a federal contractor. She received her associate's degree in 1978. Applicant married her spouse in 1987, and they have two adult children, ages 25 and 23.

Applicant started working for a large federal contractor ("A") in 2001. She became A's assistant FSO in 2005, and was its full-time FSO from 2006 to 2010. She started working for her current employer as an FSO in 2010. She has held a security clearance for 10 years. There is no evidence to show that she was ever involved in any security violations or incidents of concern, except for the SOR allegations.

In January 2014, Applicant was informed through the Joint Personnel Adjudication System (JPAS) that a company employee received a loss of jurisdiction terminating his access to classified information. Accordingly, she was required to terminate the employee's access to classified information and remove him from any classified areas upon her receipt of the loss of jurisdiction. Applicant identified the loss of jurisdiction seven days later and immediately contacted the JPAS help desk. She submitted a request to research, recertify, and upgrade the employee's clearance through JPAS asking for the security clearance to be corrected.

Applicant believed that the employee's loss of jurisdiction was an administrative error because the employee was changing jobs between federal contractors. Additionally, the loss of jurisdiction was not issued by the agency where the employee was currently working, and there was no information indicating that the employee had done something wrong because there was no incident flag.

Applicant requested assistance from the JPAS help desk to determine whether the employee's loss of jurisdiction was an administrative mistake. She confirmed that

---

*for Determining Eligibility for Access to Classified Information (AG), implemented by the DOD on September 1, 2006.*

the loss of jurisdiction did not originate from the employee's current employer, but received no further information. Applicant believed the JPAS help desk would look into the matter and call her back. Although Applicant was never told to remove the employee's access, she knew that protocol required the immediate removal of the employee's access to classified information, escort the employee out of the classified work site, and then research the issue.

Applicant followed up on her request for assistance and contacted the JPAS help desk twice over a period of two weeks. (Tr. 26) She explained that she did not contact the JPAS help desk more frequently because of her busy schedule. She also was her company's quality assurance manager and she was preparing for an audit of her facility.

In March 2014, a Defense Security Service auditor visited Applicant's facility. During the visit, Applicant discussed with the auditor and her supervisors her concerns about the possible administrative mistake causing the employee's loss of jurisdiction. The auditor did not request the immediate removal of the employee's access.

Applicant requested the recertification of the employee's eligibility in March 2014. On March 17, 2014, the Department of Defense Consolidated Adjudications Facility (DOD CAF) denied the recertification of the employee and asked Applicant to continue processing the employee's loss of jurisdiction. On March 24, 2014, Applicant emailed the auditor asking for advice on how to handle the employee's removal in JPAS. That same day, the auditor asked Applicant to "Please hold off on removing access" for the employee. (GE 1) On March 26, 2014, the employee received his eligibility for access to classified information at the top secret level.

Applicant failed to immediately remove the employee's access, and he continued to have access to classified information for another week. She explained that this was an oversight on her part due to her hectic schedule pending the facility audit.

At her hearing, Applicant's testimony was candid and forthcoming. She acknowledged that she made a mistake and failed to follow protocol when she did not immediately remove the employee's access to classified information and escort the employee from the classified work site in January 2014. Her negligence allowed an unauthorized person to access classified information during a two month period.

Applicant expressed sincere remorse and regret for her mistake and accepted full responsibility for her failure to follow protocol. Not as an excuse, but Applicant explained that she was distracted by other pressing duties, including a quality assurance audit and she failed to follow up on the removal of the employee's access. Applicant believes that she has learned an important lesson and promised to never repeat the same mistake. Following this incident, Applicant took five training courses on handling classified information. Applicant highlighted her 10 years possessing a security clearance and working as an FSO without any security violations, except for those alleged in the SOR.

Applicant submitted a strong reference letter from a prior supervisor, who served as a security manager for the Central Intelligence Agency for a period of 10 years. He then was the industrial security director for a large federal contractor. In that capacity, the reference met Applicant in 2003. She worked as an FSO and directly reported to him for a period of five years. In her reference's opinion, Applicant is trustworthy, reliable, and responsible. During the period he supervised Applicant, she was never involved in any security violations. She did an excellent job managing the company's compliance with security rules and regulations. In his opinion, Applicant's current security violation is out of character. He has full confidence in Applicant's judgment. He believes that this was an inadvertent and isolated mistake that it is unlikely to recur.

### **Policies**

Eligibility for access to classified information may be granted "only upon a finding that it is clearly consistent with the national interest to do so." Exec. Or. 10865, *Safeguarding Classified Information within Industry* § 2 (Feb. 20, 1960), as amended. The U.S. Supreme Court has recognized the substantial discretion of the Executive Branch 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).

The AG list disqualifying and mitigating conditions for evaluating a person's suitability for access to classified information. Any one disqualifying or mitigating condition is not, by itself, conclusive. However, the AG should be followed where a case can be measured against them, as they represent policy guidance governing access to classified information. Each decision must reflect a fair, impartial, and commonsense consideration of the whole person and the factors listed in AG ¶ 2(a). All available, reliable information about the person, past and present, favorable and unfavorable, must be considered.

Security clearance decisions resolve whether it is clearly consistent with the national interest to grant or continue an applicant's security clearance. The Government must prove, by substantial evidence, controverted facts alleged in the SOR. If it does, the burden shifts to the applicant to rebut, explain, extenuate, or mitigate the facts. The applicant bears the heavy burden of demonstrating that it is clearly consistent with the national interest to grant or continue his or her security clearance.

Persons with access to classified information enter into a fiduciary relationship with the Government based on trust and confidence. Thus, the Government has a compelling interest in ensuring each applicant possesses the requisite judgment, reliability, and trustworthiness of those who must protect national interest as their own. The "clearly consistent with the national interest" standard compels resolution of any reasonable doubt about an applicant's suitability for access in favor of the Government. "[S]ecurity clearance determinations should err, if they must, on the side of denials." *Egan*, 484 U.S. at 531; AG ¶ 2(b). Clearance decisions are not a determination of the loyalty of the applicant concerned. They are merely an indication that the applicant has

or has not met the strict guidelines the Government has established for issuing a clearance.

## **Analysis**

### **Guideline K, Handling Protected Information**

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.

Applicant was negligent in her duties as an FSO when she failed to immediately remove the employee's access and to escort him out of the classified work area after she received notice of the employee's loss of jurisdiction in January 2014. Additionally, she was again negligent when she failed to remove the employee's access after she was informed by the DOD CAF on March 17, 2014, to process the loss of jurisdiction. Her actions allowed an unauthorized employee access to classified information for a period of about two months.

Applicant's negligence triggers disqualifying conditions under AG ¶ 34 that raise a security concern and may be disqualifying:

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

(h) negligence or lax security habits that persist despite counseling by management.

AG ¶ 35 provides two conditions that could mitigate security concerns in this case:

(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

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

Considering the evidence as a whole, I find that mitigating conditions AG ¶¶ 35(a) and (b) apply and mitigate the security concerns in this case. Applicant should

have followed protocol to immediately remove the employee's access upon receipt of the loss of jurisdiction notice in January 2014, and after the DOD CAF told her to process the loss of jurisdiction on March 17, 2014. However, she immediately called the JPAS help desk and requested assistance researching what she perceived was an administrative mistake. She also discussed her concerns with her supervisors and sought the assistance of a DSS auditor. Ultimately, Applicant was correct and the employee's loss of jurisdiction was determined to be an administrative mistake.

Applicant acknowledged that her failure to follow protocol was a mistake and a violation of her duty to protect classified information. She expressed sincere remorse for her security violation, admitted that she was negligent, and took responsibility for her actions. Applicant's seeking additional security training, her demeanor while testifying, and her credible testimony demonstrate a renewed, positive attitude toward the discharge of her security responsibilities.

### **Whole-Person Concept**

I considered the potentially disqualifying and mitigating conditions in light of all the facts and circumstances surrounding this case, and under the whole-person concept. (AG ¶ 2(c)) 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.

Applicant, 56, has possessed a security clearance and served as an FSO for 10 years without any security incidents, except for those alleged in the SOR. There is no evidence to show that she was involved in any other security violations.

Applicant expressed remorse for her past security violations and took responsibility for her actions. She is fully aware of the serious concerns raised by her security violations. Applicant demonstrated a renewed, positive attitude toward the discharge of security responsibilities.

Considering her performance, credible contrition, and her renewed positive attitude toward the discharge of her security responsibilities, I find Applicant's past security violations are unlikely to recur and they do not cast doubt on Applicant's current reliability, trustworthiness, and judgment.

### **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.c:	For Applicant

## **Conclusion**

In light of all the circumstances presented by the record in this case, it is clearly consistent with the national interest to grant Applicant eligibility for a security clearance. Clearance is granted.

---

JUAN J. RIVERA  
Administrative Judge