KEYWORD: Security Violations; Personal Conduct

DIGEST: Applicant is a security manager for a defense contractor. She has worked with this contractor since 2000 and has held a security clearance the entire time. Applicant negligently failed to follow security requirements under the National Industrial Security Program Operating Manual. Personal conduct security concerns were raised as an issue, but none of the evidence raised separate security concerns under this guideline. Applicant has mitigated handling protected information security concerns. Clearance is granted.

CASENO: 06-21537.h1

DATE: 09/28/2007

DATE: September 28, 2007

| | | |
|---|---|---|
| In re: | ) | |
| | ) | |
| ---------- | ) | ISCR Case No. 06-21537 |
| SSN: ---------- | ) | |
| | ) | |
| Applicant for Security Clearance | ) | |

**DECISION OF ADMINISTRATIVE JUDGE**
**JACQUELINE T. WILLIAMS**

**APPEARANCES**

**FOR GOVERNMENT**
Emilio Jaksetic, Esq., Department Counsel

**FOR APPLICANT**
John F. Mardula, Esq.

**SYNOPSIS**

Applicant is a security manager for a defense contractor. She has worked with this contractor since 2000 and has held a security clearance the entire time. Applicant negligently failed to follow security requirements under the National Industrial Security Program Operating Manual. Personal conduct security concerns were raised as an issue, but none of the evidence raised separate security concerns under this guideline. Applicant has mitigated handling protected information security concerns. Clearance is granted.

## STATEMENT OF THE CASE

On May 11, 2005, Applicant executed an Electronic Questionnaire for Investigations Processing.[1] The Defense Office of Hearings and Appeals (DOHA) declined to grant a security clearance and issued a Statement of Reasons (SOR)[2] dated December 11, 2006, to Applicant, detailing the basis for its decision–security concerns raised under Guideline K (Handling Protected Information) and Guideline E (Personal Conduct) of the revised Adjudicative Guidelines (AG) issued on December 29, 2005, and implemented by the Department of Defense for SORs issued after September 1, 2006. The revised AG were provided to Applicant when the SOR was issued.

In a sworn, written statement dated December 27, 2006, Applicant responded to the SOR allegations and requested a hearing. Department Counsel was ready to proceed on July 26, 2007. The case was assigned to me on July 31, 2007. By letter dated August 6, 2007, Applicant's attorney filed a Notice of Appearance. A Notice of Hearing was issued on August 6, 2007, scheduling the hearing for August 21, 2007. The hearing was conducted as scheduled. At the hearing, the Government offered exhibits 1-4. Applicant offered exhibits A-D. All exhibits were admitted into the record without objection. At the hearing, the Government requested that administrative notice be taken of the content of three documents (I-III) about the National Industrial Security Program. There being no objection, administrative notice was taken of those facts. The transcript (Tr.) was received on September 4, 2007.

## FINDINGS OF FACT

Applicant admitted the factual allegations under subparagraph 1.a(1). Those admissions are incorporated herein as findings of fact. She denied the factual allegations under subparagraphs 1.a(2) and 2.a. After a complete and thorough review of the evidence in the record, and upon due consideration of same, I make the following findings of fact:

Applicant is 34 years old and worked as a security manager for a defense contractor since 2004. She has worked in other positions for this contractor since 2000 and held a security clearance the entire period. She has approximately two and a half years of college.

---

[1]Ex. 1 (Electronic Questionnaire for Investigations Processing, signed May 11, 2005).

[2]Pursuant to Exec. Or. 10865, *Safeguarding Classified Information within Industry* (Feb. 20, 1960), as amended, and Department of Defense Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (Jan. 2, 1992), as amended (Directive).

On December 12, 2000, Applicant was employed as a facility security officer. After retrieving a file from the safe, she failed to secure the safe, which contained classified information. This action was a violation of paragraphs 5-100, 5-300, 5-302 and/or 5-303, and 5-308b of DoD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM), January 1995. On discovering the security breach, Applicant immediately reported the incident to her manager. No classified information was compromised. As a result of this security breach, Applicant suggested rearrangement of the room so all staff "could see the containers [safes] before we left and we could see if they were opened or if they were closed."[3] A checklist was also instituted so staff would initial whether the safes were closed and secure on leaving the room.[4] Applicant was counseled on this matter and an incident report was placed in her personnel file. Applicant stated that this act was not in any way intentional, deliberate, or willful.[5]

In the late summer of 2004, Applicant was employed as the manager of the Security Office and supervised three staff members. One of her employees was the account manager and custodian of a COMSEC[6] (communications satellite) account. This employee had more than seven years of experience in managing COMSEC accounts. Applicant and her manager provided all the required resources and training in order for the custodian to adequately perform her duties. Applicant was the alternate custodian on the account. As the alternate custodian, Applicant's responsibilities were minimal.

On June 2, 2005, an Adverse Information Report was filed with the Defense Industrial Security Clearance Office to report that in the late summer of 2004, a change of custodian was initiated for the DoD material in the COMSEC account. An investigation revealed the following security violations:

- COMSEC inventories for the years 2000, 2002, 2003, and 2004 were not completed and forwarded to the NSA COR as required;
- COMSEC keying material was reported as being destroyed, but was still on hand
- COMSEC keying material was missing;
- Superseded COMSEC keying material was not destroyed after super session as required;
- COMSEC keying material was improperly stored;
- COMSEC devices were not properly safeguarded.

The investigation revealed that Applicant's performance in handling the account reflected a pattern of gross negligence and disregard of security requirements. Mismanagement of the account did not compromise security. Applicant denied the allegations in the report. Applicant, as the supervisor and alternate custodian, was unaware that the custodian employee had received several written notices and voice mails from the National Security Agency regarding the delinquent status

[3]Tr. 106.

[4]*Id*. 106-107.

[5]Applicant's Answer, dated December 27, 2006..

[6]Tr. 34.

of the account. Applicant stated that she was informally trained on this account by the custodian employee.[7] Applicant stated:

> I freely admit that while my supervisory oversight of this employee may have been considered lax, based on her level of experience, I personally did not feel that it was necessary to micro manage this account; [the employee] was an experienced security professional and COMSEC custodian.[8]

As the supervisor, Applicant was held equally responsible for the security violations of her staff member.[9] Applicant was suspended by her employer for one week without pay due to the security violations surrounding the COMSEC account.

Regarding the security violations pertaining to the COMSEC account, the Government states that Applicant violated personal conduct security standards, which are predicated on the security violations alleged under Guideline K. Allegedly, Applicant's behavior raises questions about her reliability, trustworthiness, and ability to protect classified information. Applicant denied this allegation and stated:

> My character and willingness and ability to appropriately safeguard our nation's classified information has been brought into question. At no time during either my periodic reinvestigation or the statements made in this response, have I ever demonstrated a lack of candor, dishonesty or unwillingness to comply with rules and regulations or failure to provide truthful answers during a security clearance process. My responses are truthful and candid.[10]

Applicant submitted four character letters from colleagues. They all believe she is trustworthy with unquestionable integrity. They all vouch for her character and endorse her application for a security clearance.[11]

Three coworkers, all with security clearances, testified as witnesses at the hearing. One witness stated this about the custodian issue: "She [Applicant] was trusting someone to manage the account and didn't verify that that account was being properly managed."[12] Two affidavits attesting to Applicant's character were submitted at the hearing.[13] Both witnesses believe that she is loyal to the U.S. They both endorse her application for a security clearance.

---

[7] *Id*. at 128.

[8] Applicant's Answer, note 3, *supra*.

[9] *Id*.

[10] *Id*.

[11] *Id*.

[12] Tr. 23.

[13] Ex. C (Letter, dated August 20, 2007); Ex. D (Letter, dated August 20, 2007).

Applicant is quite adept at her job. For the performance period, January 1, 2006 to December 31, 2006, Applicant received an outstanding in these categories: development, team work and process improvement, leads people, drives process improvement, and executes strategy and results. Her summary assessment was "outstanding" and her overall rating was "exceeds requirements."[14] The manager of the report noted:

> [Applicant] transitioned out of her role as Security Shared Services Manager into the role of Security Manager, International Security and Crisis Management in June 2006. Both programs were in major need of improvement and she accepted this challenge with much enthusiasm. Although [Applicant's] knowledge of managing international and crisis management programs was limited she managed to bring herself up to speed very quickly through self-study and utilization of internal company expertise and resources.[15]

In December 2004, Applicant transferred to another position with the same defense contractor. She requested a non supervisory position. In her new position, she has handled a COMSEC account for two years without any incidents.[16]

## POLICIES

Enclosure 2 of the Directive sets forth adjudicative guidelines to be considered in evaluating a person's eligibility to hold a security clearance. Included in the guidelines are disqualifying conditions (DC) and mitigating conditions (MC) applicable to each specific guideline. Additionally, each security clearance decision must be a fair and impartial commonsense decision based on the relevant and material facts and circumstances, and the whole-person concept, along with the factors listed in the Directive. Specifically these are: (1) the nature and seriousness of the conduct and surrounding circumstances; (2) the frequency and recency of the conduct; (3) the age of the applicant; (4) the motivation of the applicant, and the extent to which the conduct was negligent, willful, voluntary, or undertaken with knowledge of the consequences; (5) the absence or presence of rehabilitation; and (6) the probability that the circumstances or conduct will continue or recur in the future. Although the presence or absence of a particular condition or factor for or against clearance is not outcome determinative, the adjudicative guidelines should be followed whenever a case can be measured against this policy guidance.

The sole purpose of a security clearance determination is to decide if it is clearly consistent with the national interest to grant or continue a security clearance for an applicant.[17] The Government

---

[14]Ex. A (Individual Performance Evaluation).

[15]*Id.*

[16]Tr. 26; *see also*, Ex. B (Status of COMSEC account, dated June 18, 2007).

[17]ISCR Case No. 96-0277 (July 11, 1997) at 2.

has the burden of proving controverted facts.[18] The burden of proof is something less than a preponderance of evidence.[19] Once the government has met its burden, the burden shifts to an applicant to present evidence of refutation, extenuation, or mitigation to overcome the case against him.[20] Additionally, an applicant has the ultimate burden of persuasion to obtain a favorable clearance decision.[21]

No one has a right to a security clearance[22] and "the clearly consistent standard indicates that security clearance determinations should err, if they must, on the side of denials."[23] Any reasonable doubt about whether an applicant should be allowed access to sensitive information must be resolved in favor of protecting such sensitive information.[24] The decision to deny an individual a security clearance is not necessarily a determination as to the loyalty of an applicant.[25] It is merely an indication that the applicant has not met the strict guidelines the President and the Secretary of Defense have established for issuing a clearance.

## CONCLUSIONS

I have carefully considered all facts in evidence and the legal standards, and I reach the following conclusions.

**Handling Protected Information**

Handling protected information is always a security concern because "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." (AG ¶ 33)

Applicant admits her self-reported failure to secure a safe containing classified information. Moreover, the record reveals that with regard to the COMSEC account, security was compromised because of the custodian's negligence and disregard of security violations. As the custodian's supervisor and alternate custodian of the COMSEC account, Applicant was responsible and was suspended for one week without pay. Consequently, Handling Protected Information Disqualifying

---

[18]ISCR Case No. 97-0016 (December 31, 1997) at 3; Directive, Enclosure 3, ¶ E3.1.14.

[19]*Department of the Navy v. Egan*, 484 U.S. 518, 531 (1988).

[20]ISCR Case No. 94-1075 (August 10, 1995) at 3-4; Directive, Enclosure 3, ¶ E3.1.15.

[21]ISCR Case No. 93-1390 (January 27, 1995) at 7-8; Directive, Enclosure 3, ¶ E3.1.15.

[22]*Egan*, 484 U.S. at 531.

[23]*Id*.

[24]*Id*.; Directive, Enclosure 2, ¶ E2.2.2.

[25]Executive Order 10865 § 7.

Mitigating Conditions ¶ 34(g) (*any failure to comply with rules for the protection of classified or other sensitive information*) applies.

Various factors can mitigate handling protected information security concerns. The incident regarding the safe occurred in 2000. Applicant self-reported this incident as soon as she realized that security could have been compromised. As a matter of fact, she made suggestions, which were accepted, for rearranging the room, so others could avoid this mishap in the future. In the 2005 COMSEC incident, Applicant was the supervisor of the custodian of the account and the alternate custodian. The custodian was responsible for the daily management of the account. As her supervisor, Applicant was expected to know how the custodian was handling the work. Unbeknownst to Applicant, the custodian was negligent in handling the account and had received inquiries about the account's status without notifying Applicant. It happened once and did not recur. I conclude that Handling Protected Information Mitigating Condition ¶ 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. Applicant stated she was improperly trained to handle the COMSEC account. She relied on the custodian employee for informal training. Moreover, there is no evidence in the record to refute how much training she received. Thus, ¶ 35(c) (*the security violations were due to improper or inadequate training*) applies.

**Personal Conduct**

Personal conduct is always a security concern because "conduct involving questionable judgment, lack of candor, dishonesty, or unwillingness to comply with rules and regulations can raise questions about an individual's reliability, trustworthiness and ability to protect classified information. Of special interest is any failure to provide truthful and candid answers during the security clearance process or any other failure to cooperate with the security clearance process." (AG ¶ 15)

The old adjudicative guidelines for Personal Conduct included as a potentially disqualifying condition any "reliable, unfavorable information" involving questionable judgment, untrustworthiness, unreliability, or unwillingness to comply with rules and regulations. That general language duplicated other guidelines, such as those for Criminal Conduct or Financial Considerations.

The new adjudicative guideline for Personal Conduct has more limited language, however. Under paragraph 16(c), a disqualifying condition may arise where there is "credible adverse information in several adjudicative issue areas *that is not sufficient for an adverse determination under any other single guideline* . . . ." Paragraph 16(d) applies where there is "credible adverse information *that is not sufficient to support action under another guideline* . . . ." (Emphasis added.)

In this case, the basis for the allegations under the guideline for Personal Conduct was the evidence of breach of security violations for handling protected information. However, the security breaches are sufficient to support a basis for disqualification under another guideline. Thus, none of the evidence raises separate security concerns under the guideline for Personal Conduct.

I considered carefully all the potentially disqualifying and mitigating conditions in this case in light of the "whole person" concept, keeping in mind that any doubt as to whether access to classified information is clearly consistent with national security must be resolved in favor or the national security. Applicant accepted responsibility for both incidents involving breach of security. As to the

safe, she offered a suggestion that could benefit all staff by rearranging the room and instituting a checklist so the safe would be seen and secured upon exiting the room. She accepted responsibility for not supervising the custodian of the account more closely. Moreover, she asked to be relieved from supervising in the future. For two years she has worked in a different capacity with a COMSEC account without any security breaches. I conclude Applicant has mitigated the potential security concerns arising from handling protected information. I find that it is clearly consistent with the national interest to grant a clearance to Applicant.

## 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 (Handling Protected Information): | FOR APPLICANT |
| Subparagraph 1.a(1): | For Applicant |
| Subparagraph 1.a(2) | For Applicant |
| Paragraph 2. Guideline E (Personal Conduct): | FOR APPLICANT |
| Subparagraph 2.a: | For Applicant |

## DECISION

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

Jacqueline T. Williams
Administrative Judge