KEYWORD: Security Violations; Personal Conduct

DIGEST: Applicant is a theoretical researcher for a defense contractor. In an 18 month period from June 2002 to March 2004, she had five security violations. The violations were mostly minor and due to inadvertence. Two violations involved a failure to properly spin a safe dial lock so the lock engaged. One violation was leaving documents unattended in a kitchen area in a secure facility. Another violation was Applicant's failure to set a room alarm because Applicant believed another person was still in the room. The other violation was a failure to properly engage a room alarm that Applicant believed she had set. Applicant at all times, and since the incidents, has shown a positive attitude towards security rules and procedures. Clearance is granted.

CASENO: 06-01202.h1

DATE: 04/24/2007

DATE: April 24, 2007

In Re:	)	
-------------------	)	ISCR Case No. 06-01202
SSN: -------------	)	
Applicant for Security Clearance	)	

DECISION OF ADMINISTRATIVE JUDGE
THOMAS M. CREAN

APPEARANCES

FOR GOVERNMENT
James F. Duffy, Esq., Department Counsel

FOR APPLICANT
R. David McDowell, Esq.

SYNOPSIS

Applicant is a theoretical researcher for a defense contractor. In an 18 month period from June 2002 to March 2004, she had five security violations. The violations were mostly minor and due to inadvertence. Two violations involved a failure to properly spin a safe dial lock so the lock engaged. One violation was leaving documents unattended in a kitchen area in a secure facility. Another violation was Applicant's failure to set a room alarm because Applicant believed another person was still in the room. The other violation was a failure to properly engage a room alarm that Applicant believed she had set. Applicant at all times, and since the incidents, has shown a positive attitude towards security rules and procedures. Clearance is granted.

STATEMENT OF THE CASE

On August 30, 2006, the Defense Office of Hearings and Appeals (DOHA) issued a Statement of Reasons (SOR) detailing the basis for its decision to deny a security clearance for Applicant. The action was taken under Executive Order 10865, *Safeguarding Classified Information within Industry* (February 20, 1990), as amended, and Department of Defense Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (January 2, 1992), as amended (Directive). Applicant acknowledged receipt of the SOR on September 5, 2006. The SOR alleges security concerns under Guideline K (Security Violations) and Guideline E (Personal Conduct) of the Directive.

Applicant answered the SOR in writing on September 13, 2006. She admitted all of the allegations under both Guidelines with a detailed explanation. She requested a hearing before an administrative judge, and the request was received by DOHA on September 15, 2006. Department Counsel was prepared to proceed with the case on January 23, 2007, and the case was assigned to me on January 29, 2007. A notice of hearing was issued on February 9, 2007, and the hearing convened on February 28, 2007. Ten government exhibits, marked Government Exhibits 1-10, and the testimony of one Government witness were received without objection. Seven Applicant exhibits, marked Applicant Exhibits A-G, and the testimony of the Applicant and three Applicant witnesses were received without objection. DOHA received the transcript (Tr.) on March 19, 2007.

FINDINGS OF FACT

After a thorough review of the pleadings, transcript, and exhibits, I make the following essential findings of fact.

______Applicant is a 54-year-old theoretical researcher for a defense contractor. She has a bachelor's degree in general mathematics, a master's degree in mathematics topology with specialty in theoretical applications, and a doctorate in mathematics topology with a sub-specialty in probability and statistics from the same university. Upon receiving her doctorate in 1980, she and her then husband commenced working for a defense contractor on the west coast. She was with them for six years before she left after the birth of her daughter. While working with that defense contractor, she held a security clearance and worked with classified information. She never had a security violation. In addition, her supervisor in that position, highly praised her for sound technical skills and a sense of judgment that was greater than her years of experience. He states she had no security violations while employed by the company. He has seen her numerous times since she left the company and notes her skill, demeanor, and outlook have not changed. In 2000 after a divorce and when her daughter was 14-years-old, Applicant rejoined the work force with a defense contractor that was later purchased by her present employer. Applicant now works in a different facility than where the security violations occurred because her employer needed her specific skills at that location.[1]

Between June 2002 and March 2004, Applicant committed five security rules violations. The procedures Applicant failed to follow were all directed or required by the National Intelligence Security Procedures Manual (NISPOM) or by the contract awarded to her company by the government. The first four were considered minor violations, but the fifth was considered a major violation. Applicant was fully briefed on the security requirements of her company. She attended the briefings required for access to closed areas of the company.[2]

On June 18, 2002, Applicant removed documents no longer needed from her safe to return to document control. The document control clerk was busy so Applicant went to a kitchen area to get a coffee or soda drink. A co-worker entered the kitchen area and they engaged in conversation. Applicant left the kitchen area without retrieving the documents. About 25 minutes later, another co-worker entered the kitchen and found the classified documents.[3] Applicant's employer investigated the incident and determined there was no compromise of classified information since the kitchen was in a controlled access area of the facility. Applicant was orally counseled by her supervisor and the facility security manager and told to be more careful in handling classified documents.[4]

Applicant shared a drawer in a safe containing classified documents with a co-worker. The safe was located in a closed secure area of the facility. The safe drawer had a combination lock to secure the drawer and a handle to pull down to open the drawer. The combination lock had to be properly spun to lock the drawer and the handle. A check sheet had to be signed and initialed when unlocking and locking the combination lock and drawer. At 1715 hours on January 20, 2003, a co-worker checked Applicant's safe drawer to ensure it was locked for the night. When he pulled down on the handle, the safe opened since the combination had not been properly secured. Applicant was the last person to sign the check sheet at 1345 hours. She admitted that she inadvertently did not ensure the combination dial was spun to lock the safe. The safe was unsecured for approximately 3 hours and 30 minutes. The incident was investigated by the defense contractor and it was determined there was no compromise of classified information since the safe was located in a secure closed area accessible only to properly cleared individuals.[5] On June 17, 2003, the same safe drawer

---

[1]Tr. 92-96; 90; Government Exhibit 1 (Security Clearance Application, dated February, 6, 1998); Appellant Exhibit G (Letter, dated February 10, 2007).

[2]Government Exhibit 9 (Security Acknowledgment signed by Applicant, various dates); Government Exhibit 10 (Security briefing sign-in sheets and briefing slides, February 2003).

[3]Tr. 28-31, 100-101.

[4]Tr. 13-18; Government Exhibit 2 (Applicant's statement, dated February 16, 2005); Government Exhibit 3 (Administrative Inquiry, dated June 20, 2002).

[5]Tr. 18-20, 31-33,: Government Exhibit 2 (Applicant's statement, dated February 16, 2005); Government Exhibit 4 (Administrative Inquiry, dated January 21, 2003).

was unlocked when checked for the day at 1615 hour. Applicant was the last person to sign for opening or closing the drawer at 1600 hours. The safe had been left unsecured for approximately 15 minutes. The incident was investigated and it was determined there was no compromise of classified documents since the safe was located in the secure closed area. After both of these incidents, Applicant was counseled by the company vice-president, her direct supervisor, and the facility security manager. After the June 17, 2003, incident, Applicant was temporarily not permitted to enter the secure area without an escort.[6]

On September 26, 2003, Applicant entered a room controlled by an alarm, a cipher lock, and a card reader. Approximately 50 people assigned to the area had access to the room. When Applicant entered the room she checked to see if anyone was in the room and located another person working in an area not visible from all areas of the room. The protocol was for anyone entering the room to tell others in the room when they entered or left the room. Applicant was only in the room a few minutes. The other person in the room left in the meantime without informing Applicant he was leaving. Applicant left the room without setting the alarm because she believed the other person was still in the room. A third person entered the room seven minutes later and discovered the alarm had not been set and the room was unoccupied. Applicant admitted, and the card reader showed, that she was the last person to leave the room with the alarm not set. The incident was investigated and determined there was no compromise of classified information since the card reader showed that only cleared individuals had entered the room. Applicant received a verbal and written reprimand from her supervisor and the facility security manager.[7]

At 1710 hours on March 16, 2004, Applicant left a closed area. The area had an alarm armed from inside the room, and a cipher lock spin dial and a card reader access engaged from outside the room. Applicant signed the log as the last person to leave the room that evening. She had a co-worker check the cipher lock to be sure it was engaged. When the room was entered at 0816 hours the following day, the cipher lock was engaged but the alarm was not armed. Procedures require the alarm to be armed and activated and the cipher lock engaged. Applicant remembers activating the alarm before leaving the room. The company conducted an inquiry and determined there was no equipment malfunction and no compromise of classified information because the room had not been accessed since Applicant engaged the cipher lock. This was considered a major violation merely because of the length of time the alarm was not engaged. Applicant was again counseled by the facility security manager.[8]

---

[6]Tr. 21-23, 31-34; Government Exhibit 2 (Applicant's statement, dated February 16, 2005); Government Exhibit 5 (Administrative Inquiry, dated June 20, 2003).

[7]Tr. 34-37; Government Exhibit 2 (Applicant's statement, dated February 16, 2005); Government Exhibit 6 (Administrative Inquiry, dated September 23, 2003; Government Exhibit 7 (Notice of Violation, dated October 10, 2003).

[8]Tr. 43-50, 52-54; Government Exhibit 2 (Applicant's statement. Dated February 16, 2005); Government Exhibit 8 (Administrative inquiry, dated March 19, 2004).

Appellant received numerous awards during her tenure for her performance.[9] Her performance appraisals show she is among the best employees in her field.[10] She has received numerous letters of appreciation from the government program managers that she serves.[11]

Appellant has been concerned about security issues and problems for her company. She has questioned certain practices and recommended actions to enhance security issues for the company.[12] The vice-president of her company counseled her on security violations. He felt the security violations were caused by a lack of concentration on her part because of her busy work requirements. He discussed with her ways to avoid future violations. She has taken the necessary steps to minimize the violations in the future. He highly praised her work and her dedication.[13] The security manager of the facility where Appellant has been located since July 20, 2004, notes that there have been no security violations by Appellant since she moved to that facility.[14]

POLICIES

The President has "the authority to . . . control access to information bearing on national security and to determine whether an individual is sufficiently trustworthy to occupy a position . . . that will give that person access to such information."[15] Eligibility for a security clearance is predicated upon the applicant meeting the security guidelines contained in the Directive.[16]

The Directive sets out the adjudicative guidelines for making decisions on security clearances. Enclosure 2 of the Directive sets forth adjudicative guidelines for determining eligibility for access to classified information, and it lists the disqualifying conditions and mitigating conditions for each guideline. Each clearance decision must be fair, impartial, and a commonsense decision based on the relevant and material facts and circumstances, the whole person concept, and the factors listed in the Directive ¶ 6.3.1 through ¶ 6.3.6.

The adjudicative process is an examination of a sufficient period of a person's life to make an affirmative determination that the person is eligible for a security clearance. An administrative judge must apply the "whole person concept," and consider and carefully weigh the available, reliable

---

[9]Appellant Exhibit A (List of awards and certificates, dated, January 29, 2007).

[10]Appellant Exhibit B (Performance Appraisals, 2000 to 2006).

[11]Appellant Exhibit C (messages of appreciation, various dates).

[12]Appellant Exhibit D (Examples of security concerns, various dates).

[13]Appellant Exhibit E (Memorandum, dated April 12, 2004).

[14]Appellant Exhibit F (Letter, dated February 7, 2007).

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

[16]Directive ¶ E2.2.1.

information about the person.[17] An administrative judge should consider: (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 applicant's age and maturity at the time of the conduct; (5) the voluntariness of participation; (6) the presence or absence of rehabilitation and other pertinent behavioral changes; (7) the motivation for the conduct; (8) the potential for pressure, coercion, exploitation, or duress; and (9) the likelihood of continuation of recurrence.[18]

A person granted access to classified information enters into a special relationship with the government. The government must be able to repose a high degree of trust and confidence in those individuals to whom it grants access to classified information. The decision to deny an individual a security clearance is not necessarily a determination as to the loyalty of the applicant.[19] 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.

Initially, the Government must present evidence to establish controverted facts in the SOR that disqualify or may disqualify the Applicant from being eligible for access to classified information.[20] Thereafter, Applicant is responsible for presenting evidence to rebut, explain, extenuate, or mitigate facts.[21] An applicant "has the ultimate burden of demonstrating that it is clearly consistent with the national interest to grant or continue his security clearance."[22] The government is under no duty to present evidence to disprove any Adjudicative Guideline mitigating condition, and an Administrative Judge cannot assume or infer that any particular mitigating condition is applicable merely because the government does not present evidence to disprove that particular mitigating condition.[23]"[T]he Directive presumes there is a nexus or rational connection between proven conduct under any of the criteria listed therein and an applicant's security suitability."[24] "Any doubt as to whether access to classified information is clearly consistent with national security will be resolved in favor of the national security." [25]

Conditions that could raise a security concern and may be disqualifying, as well as those which would mitigate security concerns, pertaining to the adjudicative guidelines are set forth and discussed in the conclusions section below. Based upon a consideration of the evidence, I find the following

---

[17]*Id.*

[18]Directive ¶¶ E2.2.1.1 through E2.2.1.9.

[19]*See* Exec. Or. 10865 § 7.

[20]Directive ¶ E3.1.14.

[21]ISCR Case No. 01-20700 at 3 (App. Bd. Dec. 19, 2002); *see* Directive ¶ E3.1.15.

[22]ISCR Case No. 01-20700 at 3 (App. Bd. Dec. 19, 2002).

[23]ISCR Case No. 99-0597 (App. Bd. Dec 13, 2000).

[24]ISCR Case No. 95-0611 at 2 (App. Bd. May 2, 1996) (quoting DISCR Case No. 92-1106 (App. Bd. Oct. 7, 1993))

[25]*Egan,* 484 U.S. at 531; *see* Directive ¶ E2.2.2.

adjudicative guidelines most pertinent to the evaluation of the facts in this case:

Guideline K - Noncompliance with security regulations raises doubts about an individual's trustworthiness, willingness, and ability to safeguard classified information.

Guideline E - Personal Conduct: A security concern exists for conduct involving questionable judgment, untrustworthiness, unreliability, lack of candor, dishonesty, or unwillingness to comply with rules and regulations. Any of these characteristics in a person could indicate that the person may not properly safeguard classified information.

CONCLUSIONS

I carefully considered all of the facts in evidence and the legal standards discussed above. I reach the following conclusions regarding the allegations in the SOR.

Under Guideline K (Security Violations), a security concern exists because noncompliance with security regulations raises doubt as to an individual's trustworthiness, and willingness and ability to safeguard classified information. Appellant's five security violations raises Security Violations Disqualifying Condition Directive ¶ E2.A11.1.2.2. (*violations that are deliberate or multiple or due to negligence*). While the violations were inadvertent and not deliberate, there were five violations so there are multiple violations due to Applicant's negligence. I conclude the Security Violations Disqualifying Condition has been established.

I considered all the Security Violations Mitigating Conditions (SV MC). Since there were five violations over an 18 month period, the violations were not isolated and are frequent so SV MC Directive ¶ E2.A11.1.3.2 (*Were isolated or infrequent*) does not apply. Since there is clear evidence Applicant received proper and adequate training on security rules from her company, SV MC Directive ¶ E2.A11.1.3.3 (*Were due to improper or inadequate training*) does not apply. However, the administrative inquiries into the violations conducted by her employer and the circumstances of the violations clearly shows that they were inadvertent so SV MC Directive ¶ E2.A11.1.3.1 (*Were inadvertent*) applies. Also, the information from Applicant's facility security manager and Applicant's supervisor clearly shows that she is fully aware of security rules and is positive in applying them. The violations were mostly technical violations that occurred while Applicant was attempting to follow the rules. In two of the violations, she locked the safe but did not fully spin the locking dial to lock the safe. In another violation, she believed another person was still in the room since the person did not tell her he was leaving. She did not set the alarm believing the room was occupied. In another violation, she thought she set the room alarm for the night but misapplied the alarming procedures. She did lock the room and have it double checked by another employee. The only truly negligent act was leaving the documents in the kitchen. The evidence clearly shows Applicant is a positive force in her company in examining company practices so they comply with the security rules. She has established and demonstrated a positive attitude towards the discharge of security responsibilities, so SV MC Directive ¶ E2.A11.1.3.4 (*Demonstrate a positive attitude towards the discharge of security responsibilities*) applies. I conclude Applicant has mitigated the security concerns for security violations under Guideline K.

Under Guideline E (Personal Conduct), there is a security concern for conduct that involves questionable judgment, untrustworthiness, unreliability, or unwillingness to comply with rules and regulations. Such conduct could indicate that a person may not properly safeguard classified information. Applicant's five security violations raises Personal Conduct Disqualifying Condition Directive ¶ E2.A5.1.2.5 (*A pattern of dishonesty or rule violations*). Applicant's conduct was not dishonest but she did violate security rules, so the disqualifying condition is established. The personal conduct mitigating condition that applies to Applicant is Directive ¶ E2.A5.1.3.1 (*the information was unsubstantiated or not pertinent to a determination of judgment, trustworthiness, or reliability*). While the information substantiates the rules violations, the violations were minor, inadvertent, and due to simple negligence by Applicant while she was attempting to comply with the security rules. I conclude she has also mitigated the security concerns under personal conduct.

I carefully considered all of the circumstances in light of the "whole person" concept and apply a fair, impartial, and commonsense decision. Applicant's actions were not questionable judgment and do not indicate untrustworthiness, unreliability or an unwillingness to comply with rules and regulations. At all times, she was conscious of the security requirements and was attempting to comply with them. The violations were technical, inadvertent, and generally minor. In fact, the record shows she has good judgment, is trustworthy, and reliable. She willingly follows and embraces rules and regulations pertaining to security. I conclude Applicant is eligible 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
Subparagraph 1.a.:	For Applicant
Subparagraph 1.b.:	For Applicant
Subparagraph 1.c.:	For Applicant
Subparagraph 1.d.:	For Applicant
Subparagraph 1.e.:	For Applicant
Paragraph 2, Guideline E:	FOR APPLICANT
Subparagraph 1.a.:	For Applicant

DECISION

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

Thomas M. Crean

Administrative Judge