DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 08-10702
	)	
	)	
Applicant for Security Clearance	)	

For Government: Pamela Benson, Esquire, Department Counsel
For Applicant: *Pro Se*

September 9, 2009

Decision

DAM, Shari, Administrative Judge:

Based upon a review of the record evidence as a whole, eligibility for access to classified information is granted.

On October 16, 2007, Applicant submitted an Electronic Questionnaire for Investigations Processing (e-QIP). On March 24, 2009, the Defense Office of Hearings and Appeals (DOHA) issued to Applicant a Statement of Reasons (SOR) detailing security concerns under Guideline K (Handling Protected Information). The action was taken under Executive Order 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 revised Adjudicative Guidelines (AG) promulgated by the President on December 29, 2005, and effective within the Department of Defense for SORs issued after September 1, 2006.

On April 8, 2009, Applicant answered the SOR in writing and requested a hearing before an administrative judge. On June 4, 2009, DOHA assigned the case to me. On

June 16, 2009, DOHA issued a Notice of Hearing. The case was heard on July 8, 2009, as scheduled. Department Counsel offered Government Exhibits (GE) 1 through 4 into evidence without objection. Applicant testified, called one witness, and offered Applicant Exhibits (AE) A through E into evidence without objection. DOHA received the hearing transcript on August 13, 2009.

Procedural Matters

During the hearing, Department Counsel moved to amend the date in SOR ¶ 1.a to conform to the proof. Applicant did not object to the motion and said motion was granted. The date of said allegation is changed from May 24, 2004, to May 12, 2004. (Tr. 22-24)

Findings of Fact

In his Answer, Applicant admitted all allegations contained in the SOR. Those admissions are included in the following findings of fact:

Applicant is 39 years old and married. They have three children, ages 20, 16, and 14. He has one year of college. In August 2000, he began working as a technician specialist for a federal contractor. He works with hazardous materials. Since August 2000, his employer has disciplined him three times for his failure to comply with rules and regulations for protecting classified or sensitive materials: in May 2004, October 2004, and March 2007.

On May 12, 2004, Applicant incorrectly signed the mark out column on the security record for the laboratory, as required by his company's accessing procedures. On May 21, 2004, his manager explained the violation as follows:

> The record contains an improper mark out on May 12th which was due to the operators having accidently recorded a date in the far right time block. The first operator (Employee A) re-signed in the next block down, but the second operator [Applicant] failed to re-sign the log. We verified that [Applicant] was present at that time by checking the electronic door record which shows that he badged into the lab at 0708 on May 12th. Based on this evidence, we have verified that although the operators failed to properly complete the HML (Hazardous Material Laboratory) Security Record, they were both present and together when they unlocked the laboratory. Thus, two-man control was maintained. We will include proper sign-in procedures to our retraining efforts currently underway. (AE A at 6)

Applicant engaged in remedial counseling and received a reprimand for the violation. Later, the company changed the security procedures involved in this incident. (Tr. 30-34; AE A at 4) There is no evidence that Applicant compromised sensitive material or information as a result of his conduct.

In early 2004, Applicant's company moved the main door and key system for the laboratory. On October 26, 2004, Applicant set off the laboratory's alarm because he failed to deactivate it before entering the room. He explained that he "was not in the habit of turning the key to go through the door, because it moved from -- it used to be on the left-hand side, now it moved to a different location on the right-hand side." (Tr. 36) In late October 2004, his manager gave him a Corrective Action Plan that required him to read and re-sign the relevant security procedure, read a pertinent excerpt from the company's physical security plan, and meet with his manager to discuss security issues. His manager also required him to perform security checks at the end of the day for 30 days and to conduct a staff training session on lab security. He received another reprimand for this accessing error. (AE B; Tr. 35-37) There is no evidence that Applicant compromised sensitive material or information as a result of his conduct.

On March 20, 2007, Applicant's company changed its standard operating procedure for accessing and controlling surety locks and keys in the vault room, containing hazardous materials. (AE C) On March 23, 2007, Applicant failed to have a coworker verify with him that both locks on the vault were properly secured before leaving the area. As a result of his breach of security procedures, he was suspended from work for three days. As part of a Corrective Action Plan, he went through a one-day training program on co-person verification of securing vaults. He was also required to give a presentation to the staff on the pertinent procedures and to resecure the vault for 30 days. (AE C; Tr. 42-44) Subsequently, the company made several additional changes pertinent to securing controlled access areas.[1] (Tr. 45-46) Under those new procedures, he would not have been disciplined. (Tr. 48) There is no evidence that Applicant compromised sensitive material or information as a result of his conduct.

Applicant's supervisor's manager testified. He oversees the facility that contains the hazardous materials where Applicant works. He has held a secret security clearance for 18 years. He confirmed that subsequent to the May 2004 incident, the company changed its procedures to address Applicant's violation. Immediately prior to the October 2004 and March 2007 incidents, the company had changed procedures. (Tr. 60-61) Despite these infractions, he does not have concerns that Applicant poses a security risk. (Tr. 62) He noted that Applicant's 2009 evaluation rated Applicant as an "above average" employee. (Tr. 63) Based on Applicant's overall performance, he appointed Applicant as a trainer for other employees. (Tr. 64)

Since starting work with his employer, Applicant has received 13 performance awards. (AE E) His performance appraisals for 2005, 2006, 2007, and 2008, consistently rate him as exceeding expectations in several categories. (AE D)

Applicant testified candidly and credibly. He takes full responsibility for breaching security procedures. Since the last incident in 2007, he has tried to "slow down and pay

[1]The company disciplined three other employees for the March 23, 2007 incident. (GE 3)

better attention to detail." (Tr. 67) He is aware that if he is involved in another incident in the future, he will lose his job. (Tr. 56)

Policies

When evaluating an applicant's suitability for a security clearance, the administrative judge must consider the revised adjudicative guidelines (AG). In addition to brief introductory explanations for each guideline, the adjudicative guidelines list potentially disqualifying conditions and mitigating conditions, which are useful in evaluating an applicant's eligibility for access to classified information.

These guidelines are not inflexible rules of law. Instead, recognizing the complexities of human behavior, these guidelines are applied in conjunction with the factors listed in the adjudicative process. The administrative judge's overarching adjudicative goal is a fair, impartial, and commonsense decision. According to AG ¶ 2(c), the entire process is a conscientious scrutiny of a number of variables known as the "whole person concept." The administrative judge must consider all available, reliable information about the person, past and present, favorable and unfavorable, in making a decision.

The protection of the national security is the paramount consideration. AG ¶ 2(b) requires that "[a]ny doubt concerning personnel being considered for access to classified information will be resolved in favor of national security." In reaching this decision, I have drawn only those conclusions that are reasonable, logical, and based on the evidence contained in the record. Likewise, I have avoided drawing inferences grounded on mere speculation or conjecture.

According to Directive ¶ E3.1.14, the Government must present evidence to establish controverted facts alleged in the SOR. Under Directive ¶ E3.1.15, an "applicant is responsible for presenting witnesses and other evidence to rebut, explain, extenuate, or mitigate facts admitted by the applicant or proven by Department Counsel, and has the ultimate burden of persuasion as to obtaining a favorable clearance decision."

Section 7 of Executive Order 10865 provides that decisions shall be "in terms of the national interest and shall in no sense be a determination as to the loyalty of the applicant concerned."

A person who seeks access to classified information enters into a fiduciary relationship with the Government predicated upon trust and confidence. This relationship transcends normal duty hours and endures throughout off-duty hours. The Government reposes a high degree of trust and confidence in individuals to whom it grants access to classified information. Decisions include, by necessity, consideration of the possible risk the Applicant may deliberately or inadvertently fail to protect or safeguard classified information. Such decisions entail a certain degree of legally

permissible extrapolation as to potential, rather than actual, risk of compromise of classified information.

Analysis

Guideline K, Handling Protected Information

The security concern relating to the guideline for handling protected information is set out in AG ¶ 33:

> 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 ¶ 34 describes two conditions that could raise a security concern and may be disqualifying based on the facts of this case:

> (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.

Applicant admitted that on three occasions he failed to comply with security procedures, two of which occurred after he had been reprimanded and counseled for previous infractions. The foregoing disqualifications have been raised.

After the Government produced substantial evidence of those disqualifications, the burden shifted to Applicant to produce evidence and prove mitigation. AG ¶ 35 provides two conditions that could mitigate security concerns in this case:

> (b) the individual responded favorably to counseling or remedial security training and now demonstrates a positive attitude toward the discharge of security responsibilities; and,
>
> (c) the security violations were due to improper or inadequate training.

According to Applicant's facility manager, Applicant has responded very favorably to all security counseling and remedial training. In fact, Applicant is now training other employees in security procedures. These facts coupled with Applicant's cautious attitude in executing his security responsibilities trigger the application of AG ¶ 35(b). Two of Applicant's security breaches occurred within days of a change in the company's security procedures. After Applicant's most recent security breach, which also involved three other employees, the company changed the pertinent security procedures. These factors are sufficient evidence

to warrant the partial application of AG ¶ 35(c), as it appears that the company may have had a role in failing to properly train its employees.

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(a). They include the following:

> (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.

According to AG ¶ 2(c), the ultimate determination of whether to grant eligibility for a security clearance must include an overall commonsense judgment based upon careful consideration of the guidelines and the whole person concept.

I considered the potentially disqualifying and mitigating conditions in light of all relevant facts and circumstances surrounding this case, including the fact that sensitive materials or information were never compromised. Applicant is a 39-year-old man who breached security procedures three times within a three-year period of time. Despite that history, his employer has complete confidence in his future ability to comply with all security procedures and strongly recommends him for a security clearance. In fact, the company has asked him to train other employees in its security policies and procedures. Given Applicant's awareness that a future breach would result in the termination of his job and his diligent efforts to avoid another incident, it is most unlikely that similar incidents will recur. Overall, the record evidence leaves me without questions or doubts as to Applicant's eligibility and suitability for a security clearance. For all these reasons, I conclude Applicant mitigated the security concerns arising under Guideline K.

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 through 1.c: For Applicant

Conclusion

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

_____
SHARI DAM
Administrative Judge