KEYWORD: Security Violations; Personal Conduct

DIGEST: From approximately January 31, 2000, to February 2002, Applicant improperly permitted an uncleared employee under his supervision to access classified information. In December 2001, when U.S. mail was contaminated by anthrax, Applicant received a written reprimand from his employer after he picked up mail for his office in violation of written and verbal instructions from the federal agency directing his contract employment. Applicant failed to mitigate Guideline K and Guideline E security concerns. Clearance is denied.

CASE NO: 04-07073.h1

DATE: 06/16/2006

DATE: June 16, 2006

In Re:

SSN: ----------

Applicant for Security Clearance

ISCR Case No. 04-07073

DECISION OF ADMINISTRATIVE JUDGE

JOAN CATON ANTHONY

APPEARANCES

FOR GOVERNMENT

Daniel F. Crowley, Esq., Department Counsel

FOR APPLICANT

Pro Se

SYNOPSIS

From approximately January 31, 2000, to February 2002, Applicant improperly permitted an uncleared employee under his supervision to access classified information. In December 2001, when U.S. mail was contaminated by anthrax, Applicant received a written reprimand from his employer after he picked up mail for his office in violation of written and verbal instructions from the federal agency directing his contract employment. Applicant failed to mitigate Guideline K and Guideline E security concerns. Clearance is denied.

STATEMENT OF THE CASE

The Defense Office of Hearings and Appeals (DOHA) declined to grant or continue a security clearance for Applicant. On May 9, 2005, under the applicable Executive Order[(1)] and Department of Defense Directive,[(2)] DOHA issued a Statement of Reasons (SOR), detailing the basis for its decision-security concerns raised under Guideline K (Security Violations) and Guideline E (Personal Conduct) of the Directive. Applicant answered the SOR in writing August 22, 2005, and elected to have a hearing before an administrative judge. On February 8, 2006, the case was assigned to me. I convened a hearing on May 17, 2006, to consider whether it is clearly consistent with the national interest to grant or continue a security clearance for Applicant. The Government called one witness, introduced seven exhibits, and offered two documents for administrative notice. The Government's exhibits were identified as Ex. 1 through 7. The documents offered by the Government for administrative notice were designated Ex. I. and II. Applicant called two witnesses and introduced twelve exhibits, which were identified as Ex. A through L. The Government's exhibits and Applicant's exhibits were admitted into evidence without objections. The Government's two documents for administrative notice were admitted without objection. On May 24, 2006, DOHA received the hearing transcript (Tr.).

FINDINGS OF FACT

The SOR contains one allegation of disqualifying conduct under Guideline K, Security Violations, and two allegations of disqualifying conduct under Guideline E, Personal Conduct, of the Directive. In his answers to the SOR, Applicant admitted the Guideline K allegation and one allegation under Guideline B. His answer was silent regarding allegation

2.b. under Guideline E, which incorporated by reference allegation 1.a. under Guideline K, which he admitted. Applicant's admissions are incorporated as findings of fact.

Applicant is 52 years old, divorced, and the father of two adult children (Ex. 1.) He began his career in 1982 as an electronics bench technician. He progressed to a position supervising five other bench technicians. Over time he was promoted within the organization to an operations position and later to a position as program manager. Applicant has a trade school education in electronics and has taken business education. Additionally, he has received on-the-job training from his employers. (Tr. 75-76.)

At present Applicant works for a government contractor as an operations resource manager. In 2001 he was employed as a program manager by a government contractor. He was assigned to work in secured government facility. (Answer to SOR at 1; Tr. 54-56; Ex. 6) In that capacity he supervised approximately 68 contract employees, each of whom was required to hold a security clearance. The 68 employees were organized into five sub-groups; each sub-group was assigned its own manager/supervisor, who reported to Applicant. Additionally, there was an operations manager for the entire group who also reported to Applicant. (Tr. 70-75.)

Applicant has held a security clearance for approximately 24 years. His employers have provided him with regular security briefings. (Tr. 61; 79.) Applicant's performance appraisal for 2006 identified his completion of a unit security officer training course as one of his significant accomplishments for the year. (Ex. L at 2.)

In January 2000, Applicant hired an individual to work in his program as a security maintenance engineer, a position that required international travel and a security clearance. During the employment interview, the individual told Applicant he held a clearance while serving in the military. (Tr. 68.) The individual had recently received a general discharge (under honorable conditions) from the U.S. military. (Ex. 2; Ex. 5.) Because of the nature of the work the new hire had done in the military, Applicant assumed he would receive an expedited security clearance as a civilian. (Tr. 62-65.) On the basis of this assumption, Applicant allowed the individual to carry out assignments requiring access to classified information without the required evidence that he had been granted a security clearance.[(3)] (Tr. 64-65.)

Beginning in approximately June 2000, the new hire received assignments, as the junior member of a two-man team, that required a security clearance and access to sensitive or classified information. He carried out those assignments. In April 2001, the facility security officer (FSO), in reviewing employee folders, discovered the new hire did not have a security clearance. She notified Applicant that because the individual did not have a clearance it was necessary to remove him from his job or transfer him off the contract. Applicant asked the FSO to pursue action to obtain a security clearance for the individual. (Ex. 6; Ex. 2 at 1.)

On September 18, 2001, the FSO received notification from the Defense Security Service that it was unable to issue an interim security clearance to the individual hired by Applicant in January 2000. The FSO notified Applicant and again

advised him to remove the individual from the contract and reminded him of the requirements of the National Industrial Security Program Operating Manual (NISPOM) for a security clearance. (Ex. 2 at 3.)

In January 2002, a responsible official from the federal agency served by the contract, learning of that the individual did not have a security clearance, instructed that the individual be removed from the contract. The FSO reported this to Applicant. Applicant did not comply with the instruction, but, instead, stopped the individual's foreign travel. (Ex. 2 at 3.)

On February 8, 2002, the individual received a letter of termination from the contractor's acting program manager. He had been allowed access to sensitive or classified information without holding the requisite security clearance for approximately 24 months. (Tr. 66-67; Ex. 2 at 3.)

I take administrative notice of Sections 1-200 and 5-100 of the NISPOM, dated January 1995:

1-200. General. Contractors shall protect all classified information to which they have access or custody. A contractor performing work within the confines of a Federal installation shall safeguard classified information in accordance with this Manual and/or with the procedures of the host installation or agency.

5-100. General. Contractors shall be responsible for safeguarding classified information in their custody or under their control. Individuals are responsible for safeguarding classified information entrusted to them. The extent of protection afforded classified information shall be sufficient to reasonable foreclose the possibility of its loss or compromise.

Sections 1-200 and 5-100, dated January 1995, were in effect from January 2000 to February 2002. (Tr. 86-87.)

On November 8, 2001, Applicant went to a U.S. Post Office, which had been ordered to suspend mail delivery services because of possible anthrax contamination, and picked up two boxes of mail addressed to individuals in his office. He took the mail back to the secure federal facility where he worked, placed it in the administrative officer's office, and notified employees they could come and search the boxes for mail addressed to them. (Ex. 6 at 4-5; Tr. 48-49; 54-56.) Applicant picked up the mail in violation of official notices from the federal agency his company served as a contractor. (Ex.7 at 5-7.) Applicant stated he "was being badgered" by his staff of 60 employees to retrieve their mail. (Ex. 6 at 4.)

Applicant's action caused the federal agency's anthrax task force to decontaminate the area and to test several employees for anthrax exposure. (Ex. 7 at 2.) On December 3, 2001, Applicant received a written reprimand from his employer, which stated, in pertinent part:

This unacceptable action on your part put numerous [federal and contractor] personnel at great risk. Anthrax is not an issue to be taken lightly as proven by the death toll it has already taken. As a [name deleted] manager, we expect you to comply with all requirements applicable to your contract. This grave indiscretion on your part violates all common sense practices you are employed to uphold.

(Ex. 7 at 1.)

Applicant submitted eleven letters of character reference from managers, supervisors, and co-workers. The letters attested to Applicant's trustworthiness, reliability, and suitability for a position of trust. (Ex. A through K.)

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 occupy a position . . . that will give that person access to such information." *Id.* at 527. The President has restricted eligibility for access to classified information to United States citizens "whose personal and professional history affirmatively indicates loyalty to the United States, strength of character, trustworthiness, honesty, reliability, discretion, and sound judgment, as well as freedom from conflicting allegiances and potential for coercion, and willingness and ability to abide by regulations governing the use, handling, and protection of classified information." Exec. Or. 12968, *Access to Classified Information* § 3.1(b) (Aug. 4, 1995). Eligibility for a security clearance is predicated upon the applicant meeting the security guidelines contained in the Directive.

Enclosure 2 of the Directive sets forth personal security guidelines, as well as the disqualifying conditions (DC) and mitigating conditions (MC) under each guideline. In evaluating the security worthiness of an applicant, the

administrative judge must also assess the adjudicative process factors listed in ¶ 6.3 of the Directive. The decision to deny an individual a security clearance is not necessarily a determination as to the loyalty of the applicant. *See* Exec. Or. 10865 § 7. 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 establish, by substantial evidence, conditions in the personal or professional history of the applicant that disqualify, or may disqualify, the applicant from being eligible for access to classified information. *See Egan*, 484 U.S. at 531. The Directive presumes a nexus or rational connection between proven conduct under any of the disqualifying conditions listed in the guidelines and an applicant's security suitability. *See* ISCR Case No. 95-0611 at 2 (App. Bd. May 2, 1996).

Once the Government establishes a disqualifying condition by substantial evidence, the burden shifts to the applicant to rebut, explain, extenuate, or mitigate the facts. ISCR Case No. 01-20700 at 3 (App. Bd. Dec. 19, 2002); *see* Directive ¶ E3.1.15. 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.

CONCLUSIONS

Guideline K - Security Violations

In the SOR, DOHA alleged Applicant, a federal government contractor, improperly permitted an uncleared employee to access classified information from about January 31, 2000 through February 8, 2002 at his place of business, thereby violating paragraphs 1-200 and 5-100 of the NISPOM (DoD 5220.22-M) (¶ 1.a.).

Noncompliance with security regulations raises doubt about an individual's trustworthiness, willingness, and ability to safeguard classified information. E2.A11.1.1. In his answer to the SOR, Applicant admitted the security violation, which continued for 24 months.

Applicant's everyday work conditions required using and protecting classified information. He was a seasoned manager and responsible for supervising nearly 70 employees, all of whom required security clearances to do their work as federal contractors.

Applicant had a special duty of care to protect the classified information entrusted to him. The record shows that over many months Applicant was repeatedly advised that an employee he had hired did not have an active security clearance that was required to carry out his assigned duties. The record also shows that despite the advisories of the company's FSO, Applicant continued to permit the uncleared employee to carry out assignments for which a security clearance was required. Applicant's conduct raises a security concern under Disqualifying Condition (DC) E2.A11.1.2.1. of Guideline K, for it permitted the unauthorized disclosure of classified information.

Applicant acknowledged receiving training in security procedures required for the protection of classified information. Applicant's testimony suggested his security violation, while not deliberate, was on-going for approximately two years and was caused by negligence, thereby raising security concerns under DC E2.A11.1.2.2. of Guideline K.

We turn to an examination of applicable mitigating conditions (MC) under Guideline K. An applicant may mitigate security violation concerns if he shows the security violations were inadvertent (MC E2.A11.1.3.1.); isolated or infrequent (MC E2.A11.1.3.2.); due to improper or inadequate training (MC E2.A11.1.3.3.); or if the individual demonstrates a positive attitude toward the discharge of security responsibilities (MC E2.A11.1.3.4.).

Applicant's security violations appear to have occurred not through inadvertence but through a failure to exercise the due care required of a person entrusted with the responsibility for working with and protecting classified information. (*See* NISPOM, 5-100) His violations were not isolated or infrequent, but continued for nearly two years within a context of inattentiveness that suggests a habit or pattern of behavior. Accordingly, MC E2.A11.1.3.1. and MC E2.A11.1.3.2. do not apply to Applicant's case.

Over a span of many years, Applicant had received training in the correct handling and use of classified information. I conclude Applicant's security violations did not occur as the result of improper or inadequate training, and, therefore, MC E2.A11.1.3.3. is inapplicable to the facts of his case.

Applicant is a skilled manager whose career has been premised on work requiring that he and the people he supervised protect classified documents and information. Applicant's completion of a course that would enable him to become a unit security officer is commendable, and it demonstrates a positive attitude toward the discharge of his security responsibilities. However, while I conclude that MC E2.A11.1.3.4. is applicable in mitigation, I also conclude that, standing alone, it is of insufficient weight to overcome the disqualifying conduct alleged in the SOR. Accordingly, SOR allegation 1.a. under Guideline K of the Directive is concluded against Applicant.

Guideline E - Personal Conduct

In the SOR, DOHA alleged Applicant raised concerns under Guideline E, Personal Conduct, when he received a written reprimand from his employer on December 3, 2001, after he picked up mail from a U.S. Post Office and delivered it to a federal agency facility when mail delivery had been suspended because of possible Anthrax contamination (¶ 2.a.). DOHA also alleged that the conduct alleged in SOR 1.a. raised Personal Conduct concerns under Guideline E (¶ 2.b.).

Guideline E conduct, which involves questionable judgment, untrustworthiness, unreliability, lack of candor, dishonesty, or unwillingness to comply with rules and regulations, could indicate an applicant may not properly safeguard classified information. Directive ¶ E2.A5.1.1.

With respect to the Guideline E conduct alleged in the SOR, the Government has established its case. Applicant's conduct raises security concerns under Disqualifying Condition (DC) E2.A5.1.2.1. and DC E2.A5.1.2.5. Applicant's employer and associates at work provided reliable unfavorable information that showed his questionable judgment, untrustworthiness, and unwillingness to comply with rules and regulations. Applicant showed poor judgment when he disregarded agency instructions to suspend mail delivery and brought mail, possibly contaminated with Anthrax, back to his federal facility for distribution to the people he supervised. Applicant's conduct caused his employer to issue him a letter of reprimand, which described his actions as unacceptable, indiscreet, and in violation of common sense. This information raised security concerns under DC E2.A5.1.2.1. The information was substantiated and pertinent to a determination of Applicant's judgment, trustworthiness, and reliability. Accordingly, Guideline E mitigating condition (MC) E2.A5.1.3.1. is inapplicable and the allegation at SOR 2.a. is concluded against Applicant.

Additionally, the SFO at Applicant's employer provided reliable unfavorable information that Applicant continued, for a period of almost two years, to allow access to classified information to an employee, hired and supervised by Applicant, who did not have a security clearance. Applicant's continued refusal to act on her repeated warnings that the employee should be removed from work requiring access to classified information raises a security concern under DC E2.A5.1.2.5. and suggests a pattern of rule violations. None of the Guideline E mitigating conditions applies. The allegation at SOR 2.b. is concluded against Applicant.

In all adjudications, the protection of our national security is the paramount concern. Security clearance decisions are not intended to assign guilt or to impose further punishment for past transgressions. Rather, the objective of the security clearance process is the fair-minded, common sense assessment of a person's trustworthiness and fitness for access to classified information. Indeed, the "whole person" concept recognizes we should view a person by the totality of his or her acts and omissions, including all disqualifying and mitigating conduct. Having done so, I conclude Applicant should not be entrusted with a security clearance. In reaching my decision, I have considered the evidence as a whole, including the appropriate factors and guidelines in Department of Defense Directive, 5220.6., as amended.

FORMAL FINDINGS

The following are my conclusions as to each allegation in the SOR:

Paragraph 1. Guideline K: AGAINST APPLICANT

Subparagraph 1.a.: Against Applicant

Paragraph 2. Guideline E: AGAINST APPLICANT

Subparagraph 2.a.: Against Applicant

Subparagraph 2.b.: Against Applicant

DECISION

In light of all of the circumstances presented by the record in this case, it is not clearly consistent with the national interest to grant or continue a security clearance for Applicant. Clearance is denied.

_____

Joan Caton Anthony

Administrative Judge

1. Exec. Or. 10865, *Safeguarding Classified Information within Industry* (Feb. 20, 1960), as amended and modified.

2. Department of Defense Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (Jan. 2, 1992), as amended and modified.

3. *See* Section 2-215 of the NISPOM for the requirement that access to classified information cannot be granted until receipt of the Letter of Consent (LOC).