



DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS



In the matter of:)
)
-----) ISCR Case No. 07-01076
SSN: -----)
)
Applicant for Security Clearance)

Appearances

For Government: Melvin A. Howry, Esquire, Department Counsel
For Applicant: *Pro Se*

January 29, 2008

Decision

CURRY, Marc E., Administrative Judge:

On July 17, 2007, the Defense Office of Hearings and Appeals (DOHA) issued Applicant a Statement of Reasons (SOR) explaining why it was not clearly consistent with the national interest to grant or continue a security clearance. This action was taken under Executive Order 10865, dated February 20, 1960, as amended, and DoD Directive 5220.6, dated January 2, 1992, as amended, 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. He answered the SOR on August 3, 2007, electing to have the case decided on the written record.

Department Counsel mailed the government's file of relevant material (FORM) to Applicant on October 22, 2007. He received it on October 30, 2007. Applicant was afforded an opportunity to file objections and submit material in refutation, extenuation, or mitigation. He submitted a two-page response received by the government on November 5, 2007. The case was assigned to me on December 13, 2007. Based upon

a review of the case file, pleadings, exhibits, and testimony, eligibility for access to classified information is granted.

Findings of Fact

The SOR contains one allegation referenced under Guidelines K and E. Applicant denies that he “failed to properly secure classified material in an authorized manner in 2003,” but admits he was “counseled regarding [his] actions and given a warning” (SOR ¶ 1.a)

Applicant is a 56-year-old married man. He has no children. He served in the U.S. Navy from 1973 through his retirement in 1993 (Item 4 at 2). He has an associate’s degree in forestry/wildlife management earned in 1990.

Since 1995, he has worked as a project manager at a defense contractor. His duties include, among other things, missile system maintenance for Navy ships. The defense contractor maintains two coastal offices on opposite sides of the country. Applicant worked in the satellite office located across the country from the main office.

In December 2003, Applicant was tasked with overseeing the upgrade of a ship’s missile system. Such projects normally take four weeks to complete (Item 6 at 3). In this case, Applicant only had two weeks to complete the project before the ship deployed. The upgrade project involved removing the obsolete missile system, disassembling it, and removing it from the ship.

The obsolete missile system consisted of nine components. Eight of its nine components were labeled confidential. The ninth component was unlabeled. Typically, when old, classified components were replaced, the ship’s supply officer was responsible for transferring them to the defense contractor’s main office. In this case, the supply officer was on leave, and Applicant was unaware of any backup transfer procedures (Item 6 at 3). He was afraid that the parts would be lost or misplaced if he left them on the ship after it deployed (Item 6 at 3).

Applicant decided to transfer the parts himself. He contacted his employer’s main office to request an authorized courier to retrieve the components (Response to FORM, at 1). He never received a response. As the deployment date grew nearer, he decided to remove the components himself. He wrapped the parts in two separate, small brown paper bags, taped and marked them “confidential,” completed a DD Form 1149, a form documenting the transfer of government material from the ship’s custody,¹ and removed the components from the ship (Item 5 at 3). After removing them, he placed them in his office safe which was certified to hold classified items (Response to FORM; Item 6 at 4).

¹The FORM 1149 was signed by a Navy Petty Officer.

Applicant then contacted his company's fleet technical support center at the main office for instructions on disposing of the components. Again, he did not receive a response (Item 6 at 3).

Approximately eight months later during an annual self-inspection in July 2004, Applicant disclosed that he was storing the components in the safe, prompting an investigation (Item 5 at 1). Before then, he had never informed his supervisor that the components were in the safe. Consequently, Applicant was counseled regarding his actions and given a warning (Item 3 at 1).

According to the employer's adverse information report, the components may have been declassified at the time Applicant removed them from the ship (Item 5 at 2, ¶3). There is no record evidence documenting whether this issue was ever resolved. The record evidence regarding whether the material was classified when Applicant removed it from the ship is inconclusive. Absent conclusive evidence of whether the components were classified, I accept Applicant's contention that no compromise of classified information occurred.

Applicant had never been reprimanded for his work performance before this incident. He worked for his employer for another 10 months through May 2005 without incident. After briefly being furloughed in March 2006 because of lack of work, he returned in April 2006 to work on another project (Item 6 at 4).

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 common sense 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.

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

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 an 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.

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.” See *also* EO 12968, Section 3.1(b) (listing multiple prerequisites for access to classified or sensitive information).

Analysis

Guideline K - Handling Protected Information

Under this guideline, “deliberate or negligent failure to comply with rules and regulations 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). Here, the SOR alleges Applicant failed to secure classified material when removing it from a ship. Applicant denies the allegation, and evidence upon which the government’s allegation is based (Item 5) is inconclusive. The government has not met its burden because it failed to prove the materials involved were classified. Therefore, I conclude there are no Guideline K security concerns.

Guideline E - Personal Conduct

The government’s failure to establish the components were classified does not end the security clearance scrutiny. When he began working on the project, Applicant clearly believed the components were classified, yet failed to remove them from the ship consistent with regulations governing the handling of classified material (*See generally*, DoD 5220.22-M ¶¶ 2-100, 5-100, 5-202, and 5-204). Moreover, although he made two requests for instructions to his main office, and received no response, he reached the decision to store the material in the office safe without informing his immediate supervisor.

This raises Personal Conduct security concerns. Under this guideline, “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” (AG ¶ 15). The disqualifying condition most pertinent to Applicant’s case is AG ¶ 16 (d)(1), “untrustworthy or unreliable behavior to include breach of client confidentiality, release of proprietary information, unauthorized release of sensitive corporate or other government protected information.”

The incident occurred more than four years ago. Also, he was operating under extreme time pressure. Although disposing of obsolete parts was normally not his responsibility, he had to handle the task because the designated supply officer was on leave at the time. No compromise of classified information occurred. Before this incident, he had never made any similar judgment lapses while performing his job duties, and he has not made any since then. As punishment, he was merely given a warning, and counseled. AG ¶ 17(c), “the offense is so minor, or so much time has passed, or the behavior is so infrequent, or it happened under such unique circumstances that it is unlikely to recur and does not cast doubt on the individual’s reliability, trustworthiness, or good judgment,” applies.

Applicant has mitigated the personal conduct security concern.

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 the circumstances. The administrative judge should consider the nine adjudicative process factors listed at AG ¶ 2(a): “(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) 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.” Under AG ¶ 2(c), the ultimate determination of whether to grant eligibility for a security clearance must be an overall commonsense judgment based upon careful consideration of the guidelines and the whole person concept.

Here, the nature and seriousness of the conduct were minimal. The material Applicant removed from the ship may not have been classified, and there is no evidence any compromise occurred. He was merely issued a warning, and allowed to continue working. Moreover, assuming for the sake of argument that the material was classified, Applicant, by removing it from the ship before it deployed, and later attempting to contact his company’s fleet technician, was performing his job duties in a good-faith manner.

The unique nature of these circumstances renders the likelihood of recurrence minimal. Applicant was working on a short deadline, and was faced with an unanticipated situation, because the supply officer, who normally disposed of the obsolete equipment, was on leave. Although he probably should have contacted his supervisor before removing the items, or at minimum, talked with him after the removal, he had never committed such judgment lapses in the past, and has not committed any since the incident. Upon evaluating this case in the context of the whole person concept, I conclude Applicant has mitigated the security concerns. Clearance is granted.

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
Paragraph 2, Guideline E:	FOR APPLICANT
Subparagraph 2.a:	For Applicant

Conclusion

In light of all of 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. Eligibility for access to classified information is granted.

MARC E. CURRY
Administrative Judge