



DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS



In the matter of:)	
)	
-----)	ISCR Case No. 07-05761
SSN: -----)	
)	
Applicant for Security Clearance)	

Appearances

For Government: Jennifer I. Goldstein, Esquire, Department Counsel
For Applicant: B. Daniel Lynch, Esquire

August 7, 2008

Decision

MOGUL, Martin H., Administrative Judge:

Applicant submitted his Security Clearance Application (SF 86), on November 7, 2006. On December 13, 2007, the Defense Office of Hearings and Appeals (DOHA) issued a Statement of Reasons (SOR) detailing the security concerns under Guidelines K and E for Applicant. 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.

Applicant responded to the SOR (RSOR) in writing on April 4, 2008, and requested a hearing before an Administrative Judge. I received the case assignment on May 14, 2008. DOHA issued a Notice of Hearing on June 11, 2008, and I convened the hearing on June 26, 2008. The Government offered Exhibits 1 through 4, which were received without objection. Applicant testified on his own behalf and three other witnesses testified on behalf of Applicant. Through counsel, he submitted Exhibits A through E, which were entered without objection. DOHA received the transcript of the

hearing (Tr) on July 7, 2008. Based upon a review of the case file, pleadings, exhibits, and testimony, eligibility for access to classified information is denied.

Findings of Fact

After a complete and thorough review of the evidence in the record, including Applicant's Answer to the SOR, the admitted documents, and the testimony of Applicant and the additional witnesses, and upon due consideration of that evidence, I make the following findings of fact:

Applicant is 54 years old. He is married, and he has two children. He has received two Bachelor of Science degrees and one Master's Degree in electrical engineering.

Applicant works as an electrical engineer for a defense contractor, and he seeks a DoD security clearance in connection with his employment in the defense sector.

Paragraph 1 (Guideline K - Handling Protected Information)

The SOR lists 4 allegations under Adjudicative Guideline K. All of the allegations will be discussed in the same order as they were listed in the SOR:

1.a. On or about March 3, 2006, Applicant received a first warning letter from his employer after a security inspection revealed that Applicant had failed to secure a classified container in an approved manner.

In the Final Report of Investigation (Exhibit 4), the investigator stated that Applicant's safe was not secured because the "lock bar [was] not in place." An examination of a sample of the material in the safe determined it to be DoD Secret. The investigator indicated in his report that Applicant informed him that he had "worked late and forgot to secure the cabinet." Compromise was considered extremely minimal. However, it could not be ruled out, and therefore Applicant received the Security Violation.

During Applicant's testimony, he conceded that he had inadvertently left open his safe (tr at 72).

1.b. The security violation, summarized in subparagraph 1.a., above is a violation of DoD 5520.22-M, the National Security Manual, dated February 28, 2006, and DoD National Industria Program Operating Manual (NISPOM) Supplement, dated April 1, 2004.

1.c. On or about November 29, 2006, Applicant received a second warning letter from his employer after a security inspection revealed that Applicant had failed to secure classified material and media, some of which had their specific classification markings crossed out, in an approved container.

In the second Final Report of Investigation, dated February 7, 2007, (Exhibit 4), the investigator stated that Applicant “failed to store media and two binders marked as Secret/SAR/SJS in a SJS approved container within an SJS approved area. [Applicant] . . . also failed to conduct proper downgrading procedures and did not take into consideration the media was originated on a SAR system. [Applicant] . . . instead downgraded a disk by marking out the DJS/SAR with a black marker.”

The investigator indicated in his report that “because the same DoD security container was inadvertently left unsecured on 3 March 2006, and the fact it could not be determined when the binders were placed in the DoD container the potential for compromise cannot be ruled out.”

Applicant testified that he had removed SAR or Special Access Required from one of the disks he placed in his file because “I was told that the information [on the disk] was not SAR, and at the time I didn’t understand the rules and regulations of the markings, cause on hard copy documents, if we knew something’s not SAR, we can cross that out.” (Tr at 75-76).

1.d. The security violation, summarized in subparagraph 1.c., above is a violation of DoD 5520.22-M, the National Security Manual, dated February 28, 2006, and DoD National Industria Program Operating Manual (NISPOM) Supplement, dated April 1, 2004.

While it was not alleged in the SOR, it was revealed during the hearing that Applicant has had two additional security violations. Applicant revealed that in approximately 1990 he was cited and counseled for leaving his safe open (Tr at 85).

Applicant’s supervisor from January 2004 through November 2007 also revealed during his testimony that an additional warning letter was issued to Applicant in June 2005, although apparently it was no longer in the file, and therefore was not included in the SOR (Tr at 30-32). This warning was issued to Applicant and two or three other individuals who shared a safe, because it was determined that special access material was in a safe not authorized for these documents. Applicant was the primary custodian of the safe at the time these documents were located to be incorrectly stored.

Applicant’s supervisor also testified that there is a web based annual security certification that all program access individuals must complete, and that covers such areas as handling of special access materials and storing them in proper containers (Tr at 34). Finally, this supervisor submitted a character letter recommending Applicant retain his security clearance (Exhibit A).

Paragraph 2 (Guideline E - Personal Conduct)

2.a. The Government alleges that Applicant’s security violation, as alleged in paragraph 1, above exhibits questionable judgement and unwillingness to comply with rules and regulations.

Mitigation

Applicant testified that since his last warning he has better organized, cataloged his safe and drastically reduced the number of document in it so he knows exactly what documents are in the safe to limit the likelihood of having inappropriate documents in it (Tr at 91). He also locks his safe now every time he removes a classified document rather than waiting until he has finished with the document and replaced it (Tr at 92 -93).

Finally, two additional witnesses testified on behalf of Applicant, his daughter and his wife. His daughter characterized her father as a very responsible person, who never revealed anything inappropriate about his work to her. Applicant's wife of 27 years testified that her husband is honorable, truthful, and extremely reliable. Applicant also offered into evidence three additional character letters from individuals who know or have known him in his professional or private life (Exhibit D). They all were extremely laudatory in describing Applicant as careful, honest, intelligent, and reliable.

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 over-arching 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 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.

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

With respect to Guideline K, the Government has established its case. Applicant's improper handling of secured information, which resulted in three letters of warning during the period from 2005 through 2007, is of great concern to the Government. His storing material improperly in his safe, leaving his safe unsecured and changing the classification on a secured disk comes within the Disqualifying Conditions (DC) 34. (b) (collecting or storing classified or other protected information in an unauthorized location), (g) (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).

In reviewing the Mitigating Conditions (MC) under 35., I find that Applicant's three violations, that occurred within the last three years, are too recent and too frequent to conclude that such conduct will not recur again. Based on Applicant's former supervisor's testimony about the training that employees receive, I can not conclude that Applicant received improper or inadequate training. While MC (b) (the individual now demonstrates a positive attitude toward the discharge of security responsibilities) can be argued to be applicable, I do not find it controlling because it is too recent from the time of the violations to establish the security significance of this mitigating factor.

In this case, the Government has met its burden of proving by substantial evidence that Applicant has negligently failed to comply with rules and regulations for protecting classified information, which raises doubt about his trustworthiness, judgement, reliability and willingness and ability to safeguard such information. I find that these events happened too recently and too frequently for Applicant to overcome the Government's case against him at this time. Accordingly, Paragraph 1 Guideline K of the SOR is concluded against Applicant.

Guideline E - Personal Conduct

With respect to Guideline E, the evidence establishes that Applicant's conduct comes under DC (d) (3) because his pattern of rules violations supports a whole-person assessment of untrustworthiness, unreliability, and unwillingness to comply with rules and regulations

I resolve Paragraph 2, Guideline E, against Applicant.

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.

I have considered the potentially disqualifying and mitigating conditions under Guidelines K and E, in light of all the facts and circumstances surrounding this case. Based on all of the reasons cited above, including the recency and frequency of rules violations, I find that the record evidence leaves me with sufficient questions and doubts as to Applicant's eligibility and suitability for a security clearance under the whole person concept. For all these reasons, I conclude that at this time, Applicant has not mitigated the security concerns.

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:	AGAINST APPLICANT
Subparagraph 1.a:	Against Applicant
Subparagraph 1.b:	Against Applicant
Subparagraph 1.c:	Against Applicant
Subparagraph 1.d:	Against Applicant
Subparagraph 1.e:	Against Applicant
Paragraph 2, Guideline E:	AGAINST APPLICANT

Conclusion

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 Applicant eligibility for a security clearance. Eligibility for access to classified information is denied.

Martin H. Mogul
Administrative Judge