

KEYWORD: Security Violations; Personal Conduct

DIGEST: Applicant was involved in several security violations between 1989 and 1994 that were caused by her failure to accurately document and handle classified information. Applicant failed to mitigate the resulting security violations and personal conduct security concerns. Clearance is denied.

CASENO: 02-06951.h1

DATE: 07/28/2004

DATE: July 28, 2004

In re:

SSN: -----

Applicant for Security Clearance

CR Case No. 02-06951

DECISION OF ADMINISTRATIVE JUDGE

JAMES A. YOUNG

APPEARANCES

FOR GOVERNMENT

Jennifer I. Campbell, Esq., Department Counsel

FOR APPLICANT

Pro Se

SYNOPSIS

Applicant was involved in several security violations between 1989 and 1994 that were caused by her failure to accurately document and handle classified information. Applicant failed to mitigate the resulting security violations and personal conduct 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 6 January 2004, DOHA issued a Statement of Reasons⁽¹⁾ (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 on 22 January 2004 and elected to have a hearing before an administrative judge. The case was assigned to me on 7 April 2004. On 25 May 2004, I convened a hearing to consider whether it is clearly consistent with the national interest to grant or continue a security clearance for Applicant. DOHA received the hearing transcript (Tr.) on 3 June 2004.

FINDINGS OF FACT

Applicant is a 42-year-old employee of a defense contractor. She handles the incoming and outgoing financial documentation, receives funding, and tracks costs. She is single and raising two children. She has worked for her current employer for approximately 16 months and held an interim clearance for eight of those months. She had no security violations or infractions while working for this company. Tr. 57-58.

Applicant worked for a different defense contractor from 1989 until 1997. In 1989, Applicant was responsible for

mailing classified documents to another defense contractor. She addressed the envelope to a post office box belonging to a different division of the defense contractor than the division to which the documents were intended to go. Ex. 3 at 46. The documents should have been delivered directly to a designated person. *National Industrial Security Operating Program Operating Manual* (NISPOM) ¶ 5-204. The documents were eventually delivered to a cleared person and there was no unauthorized disclosure of classified information. No corrective action was taken against Applicant other than her supervisor discussing the error with her. Ex. 3 at 43.

In February 1990, Applicant was working as a secretary typing documents for engineers. She held a secret clearance then. After the documents were typed, the engineers, with the concurrence of the program sponsor, determined that the combination of secret and unclassified information in the documents required they be classified top secret. Applicant was in no way responsible for the incident nor could she have prevented it. Tr. 26; Ex. D.

In April 1990, Applicant and a co-worker made 30 copies of a classified document and prepared 18 packages for mailing. When she arrived at the post office, Applicant discovered she only had 17 packages. After returning to the work facility, Applicant and the co-worker "searched for the missing document in the copy room, the supply room (where the packaging was done), and in each of their respective offices." Ex. 3 at 35. They could not find the document, so incorrectly believed they had put two of the documents into one of the packages that had been mailed. Another cleared co-worker found the documents in the supply room three days later. Uncleared cleaning personnel had access to the room during the period the document was missing. *Id.* at 36.

In September 1993, while preparing for an inspection of the defense contractor's security procedures, members of the engineering division discovered that two documents were missing. Following the inspection, a third document was discovered to be missing. Ex. 3 at 25. A determination was made that one of the documents had been shredded and the other two had never been created. In January 1994, Applicant was reprimanded for failing to maintain accurate accountability records for the three documents. Ex. 4 at 2-3.

In 1997, Applicant was a program security officer but also served about eight hours a week as the facility security officer (FSO) at an off-site location. The company was preparing for a security inspection. There was a considerable amount of work to be done at the off-site facility before it would be ready for a security inspection. Applicant complained to her superiors about her working space at the off-site location. She claimed she had neither the necessary space nor facilities to perform her duties appropriately. Her supervisors declined to remedy the situation, claiming the facilities were adequate. On 20 March 1997, Applicant sent an e-mail to a superior describing her frustration with the available working space at the off-site facility. She asserted the safe room was being used as a storage facility filled with computer boxes, wall boards, and wall hangings. She ended her e-mail with the following:

I understand that space is limited, but where do you draw the line.

I refuse to work in these conditions. Maybe attention will be given to security when we fail.

HELP!!!

Rather than view this as a cry for assistance, Applicant's bosses viewed the e-mail as a threat to purposely fail the inspection if she did not get a "nicer office." Tr. 20. The defense contractor terminated her as the facility security officer. An audit of the records in the off-site facility revealed "a considerable amount of chaos in the documents and receipt records." Tr. 21. The "document control situation was a terrible mess." *Id.*

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 personnel 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 committed three security violations (¶¶ 1.a, 1.c, 1.d) and was involved in a security incident (¶1.b). Noncompliance with security regulations raises doubt about an applicant's trustworthiness, willingness, and ability to safeguard classified information. Directive ¶ E2.A11.1.1.

The Government established by substantial evidence each of the allegations in ¶ 1. Applicant was involved in multiple security violations due to negligence. DC E2. A11.1.2.2. Although a security incident may have occurred in February 1990 when Applicant typed documents that were later classified at a higher level, it is clear from the evidence Applicant did nothing wrong and cannot be faulted for the incident. I find for Applicant on ¶ 1.b.

All of the violations were inadvertent. MC E2.A11.1.3.1. Applicant seems to have been overwhelmed by her duties and unable to manage the documentation and filing responsibilities necessary for her position with the company. The established security violations, coupled with evidence that the off-site facility's "document control situation was a terrible mess," demonstrate Applicant's inability to safeguard classified information. I find against Applicant on ¶¶ 1.a, 1.c, and 1.d.

Guideline E-Personal Conduct

In the SOR, DOHA alleged Applicant was removed from duties as the FSO, in part, because she refused to work in conditions that existed prior to a security inspection (¶ 2.a) and the allegations of security violations from ¶ 1 (¶ 2.b). Conduct involving questionable judgment, untrustworthiness, unreliability, lack of candor, dishonesty, or unwillingness to comply with rules and regulations could indicate that the applicant may not properly safeguard classified information. Directive ¶ E2.A5.1.1.

The Government established by substantial evidence and Applicant's admissions each of the allegations in the SOR. Although Applicant was removed from her duties as FSO, I conclude she was not threatening her supervisors with failing the security inspection if she did not get a better office. She was frustrated and asking for help so that she could better do her job. I find for Applicant on ¶ 2.a. Applicant's involvement in other security violations as noted in ¶¶ 1.a., 1.c, and 1.d, is reliable, unfavorable information showing her unreliability concerning the handling of classified information (DC E2.A5.1.2.1) and a pattern of rules violations (DC E2.A5.1.2.5). None of the mitigating conditions apply. I find against Applicant on ¶ 2.b.

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

Subparagraph 1.b: For Applicant

Subparagraph 1.c: Against Applicant

Subparagraph 1.d: Against Applicant

Paragraph 2. Guideline E: AGAINST APPLICANT

Subparagraph 2.a: For 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

James A. Young

Administrative Judge

1. Pursuant to Exec. Or. 10865, *Safeguarding Classified Information within Industry* (Feb. 20, 1960), as amended and modified, and Department of Defense Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (Jan. 2, 1992), as amended and modified (Directive).