KEYWORD: Information Technology; Personal Conduct

DIGEST: Applicant successfully mitigated disqualifying conduct under Guidelines M and E of the Directive. Clearance is granted.

CASENO: 03-12059.h1

DATE: 02/13/2006

DATE: February 13, 2006

In Re:

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

Applicant for Security Clearance

ISCR Case No. 03-12059

DECISION OF ADMINISTRATIVE JUDGE

JOAN CATON ANTHONY

APPEARANCES

FOR GOVERNMENT

Julie R. Edmunds, Esq., Department Counsel

FOR APPLICANT

Leslie McAdoo, Esq.

SYNOPSIS

Applicant successfully mitigated disqualifying conduct under Guidelines M and E of the Directive. Clearance is granted.

STATEMENT OF THE CASE

The Defense Office of Hearings and Appeals (DOHA) declined to grant or continue a security clearance for Applicant. On October 7, 2004, 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 M (Misuse of Information Technology Systems) and Guideline E (Personal Conduct)of the Directive. On October 19, 2004, Applicant submitted an answer to the SOR. By letter dated February 11, 2005, Applicant elected to have a hearing before an administrative judge. The case was assigned to another administrative judge for hearing on April 4, 2005. On June 20, 2005, the case was assigned to me when regional assignments were rotated. On November 14, 2005, I convened a hearing to consider whether it is clearly consistent with the national interest to grant or continue a security clearance for Applicant. The Government called no witnesses and introduced five exhibits, which were identified and numbered Ex. 1 through 5. Applicant called no witnesses and introduced four exhibits, which were identified as Exs. A, B, C, and D. All exhibits were admitted to the record without objection. DOHA received the transcript (Tr.) of the proceeding on December 1, 2005.

FINDINGS OF FACT

The SOR in this case contains two allegations of disqualifying conduct under Guideline M, Misuse of Information Technology Systems, and three allegations of disqualifying conduct under Guideline E, Personal Conduct. In his answer to the SOR Applicant admitted two allegations, denied two allegations, and admitted and denied one allegation. Applicant's admissions are incorporated as findings of fact.

Applicant is 38 years old, married, and the father of two small children. He is employed as a Lead Engineer by a government contractor.

Applicant is a naturalized U.S. citizen. He was born in Country A, but his nationality and his first language were derived from Country B. Applicant lived in Country A until he was approximately 21 years old. He then moved to Country B, where he lived for approximately two years and attended technical school. He emigrated to the U.S. in 1992. He learned English after arriving in the U.S. (Ex. 1; Tr. 22-24.)

In 1994, Applicant acquired a job in building maintenance with Company 1. From 1994 to 2000, Applicant's performance of his duties was unremarkable, and he carried out his responsibilities without incident. On his own time, he studied two evenings a week for about three years to become a steam engineer 3rd class. He earned his 3rd class license in early 2001. (Tr. 30;57-58.)

In about 2000, Applicant's employer transferred him to a new building, where he was supervised by a Chief Engineer who "didn't like foreigners with accents." (Tr 29-30.) The Chief Engineer asked Applicant "when [he] was going to get licensed to go somewhere else." (Tr.30-32.)

The Chief Engineer had a government computer in his office that Applicant and several other employees were authorized to use. Applicant, whose experience with computers was limited, used the computer in the Chief Engineer's office to access his e-mail. In May 2000, Applicant logged on to the computer three times to review his e-mail. He opened e-mails addressed to him and discovered they contained pornographic material. He tried to close and delete the pornographic web sites. The Chief Engineer found out about Applicant's actions and issued him a letter of counseling. (Ex. 2.) Applicant denied intentionally looking for pornographic web sites on the computer. (Tr. 34-35.)

Most of Applicant's supervisors and co-workers were men. In the work culture, salesmen hoping to obtain orders from the engineers would bring them "girlie" calendars and magazines. These calendars and magazines were often displayed in the engineers' offices. (Tr. 35-37.)

In March 2001, Applicant's supervisor, the Chief Engineer, went on vacation. Applicant, along with other authorized employees, went into the Chief Engineer's office to use the computer and access their e-mails. When the Chief Engineer returned from his vacation, he alleged Applicant had entered pornographic web sites again. (Tr. 38; Ex. C.) Applicant again denied intentionally entering pornographic web sites. In his answer to the SOR, Applicant said he was on duty in the building and not at the computer when the alleged misuse occurred. (Answer to SOR at 1.) A company manager also alleged Applicant had "girlie" calendars which were hung in the Chief Engineer's office. Applicant denied the calendars were his or that he had hung them in the Chief Engineer's office. (Ex. 3;36-38.)

The Chief Engineer did not believe Applicant's denials. He told Applicant he couldn't continue to work for the company. He suggested Applicant needed "to take another direction." (Tr. 38-39.)

Applicant, who had recently acquired 3rd class engineer's license, had been actively seeking a better-paying job. He told the Chief Engineer he would leave rather than admit to transgressions he had not committed. Applicant cleaned out his desk and left the company. He received all pay, benefits, vacation time, and personal days he had earned. The employer processed a form indicating Applicant had been fired. Applicant thought he had resigned. Two weeks later he had a new job with his present employer (Company 2). (Tr. 39-40; Ex. 4.)

Applicant went to work for Company 2 in April 2001. In his current job with Company 2, Applicant has authorized access to computers. Applicant's current employer has not raised issues regarding access to pornographic web sites from official company computers. (Tr. 41.)

In his new job with Company 2, there was a personnel shortage that made it necessary for Applicant to work 16-hour shifts each day for about six weeks. Applicant's duties required him to physically check the temperature of the building's hot water tanks once each shift and to note the temperature and time on a tank log sheet. On one occasion, in order to avoid logging in the temperature of the water tanks twice in one shift, Applicant did not accurately report the times he checked the tanks. At 2:30 pm on a given day, Applicant filled in log sheets for two tanks at 3:10 pm and 4:00 pm. On March 25, 2002, his supervisor issued him a letter warning that it was a very serious matter, punishable by time off without pay, and possible dismissal, to inaccurately fill out the log sheets. (Ex. 5; Tr. 41-44.)

In April 2001, Applicant completed a Questionnaire for National Security Positions (SF-86). Question 22 on the SF-86 asks if an applicant has ever been fired from a job; quit a job after being told he or she would be fired; left a job by mutual agreement following allegations of misconduct; left a job by mutual agreement following allegations of unsatisfactory performance; or left a job for other reasons under unfavorable circumstances. Applicant responded "no" to Question 22.

Applicant testified he did not think he had been fired from his job in March 2001, and when he saw Question 22 he read only the part about being fired from a job and answered it, correctly in his mind, as "No." (Tr. 45-46.) On September 17, 2002, Applicant was interviewed by an agent of the Defense Security Service (DSS). Before the subject of his employment history was raised by the investigator, Applicant raised the issue himself. He told the security investigator he thought he had resigned his job with Company 1, but later learned his employer had reported it had terminated him. (Ex. C.)[(3)] Applicant stated his omission was the result of oversight, and he did not intend to hide or fail to disclose information about his job termination (Ex. C.) At his hearing he opined he should have answered Question 22 by stating he had left the job by mutual agreement. (Tr. 46-48.) Applicant's former employer confirmed that Applicant had been terminated when interviewed by the special agent on October 23, 2002. A review of Applicant's employment documents by the DSS in January 2003 indicated his employer had submitted paper work terminating him from his job. (Ex. D; Ex. 4.)

The supervisor at Company 2 who issued Applicant a letter of warning on March 25, 2002, also submitted a letter of character reference for Applicant on October 18, 2004. (Ex. A) The letter of character reference reads, in pertinent part, as follows:

[Applicant] did in fact make the mistake that I documented in a letter to him The action was a single incident that has not been repeated since. In fact, over the last 30 months he has become one of my most knowledgeable and trustworthy building engineers.

As the Chief Engineer for some of the [government agency's] most critical facilities, I understand the requirement for employing trustworthy individuals. It is my opinion, based on his total past performance, that [Applicant] exemplifies the type of Engineer needed to maintain the operations of mechanical equipment at the [government agency] or any other facility. On countless occasions, [Applicant] has given up his family life to maintain this facility when we were short handed and needed assistance. [Government Contractor] recently promoted [Applicant] to a Lead Engineer. The Lead Engineer is a position of trust and confidence in which [Government Contractor] and the Government must agree. . . .

In conclusion I have watched [Applicant] progress through the ranks into a mature respected engineer. Yes, he made a mistake years ago and was disciplined. On March 25, 2002 I believed he was of value to this facility, his company, and the Government. Since that date he has reinforced that he is a valuable asset to the Government, this facility, and [Government Contractor]. I believe [Applicant] to be trustworthy and honest. . . .

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 and mitigating conditions 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 M - Misuse of Information Technology Systems

In the SOR, DOHA alleged under Guideline M of the Directive that Applicant accessed pornographic Internet web sites in May 2000 on his employer's computer, in violation of company rules, procedures and guidelines, and that he was counseled by his employer about this conduct (¶ 1.a.); and that Applicant accessed pornographic Internet web sites on

his employer's computer in March 2001, conduct which was specifically prohibited by company rules, procedures, and guidelines and for which he was fired by his employer on March 23, 2001 (¶ 1.b.).

Applicant's two unauthorized entries into his employer's technology system in 2000 and 2001, in violation of his employer's policy and procedures, raise security concerns under Disqualifying Condition (DC) E2.A.13.1.2.1. of Guideline M. The record evidence and Applicant's credible testimony indicate his misuse of his employer's computer system occurred while he was attempting to access his e-mail account, which he was authorized by his employer to do, and that on three occasions in 2000 and at least one occasion in 2001 he inadvertently accessed pornographic web sites, which he closed and tried to delete. Applicant's misuse of his employer's computer system was not recent, nor was it significant. He supplied credible testimony to show his conduct was unintentional and inadvertent. Accordingly, Mitigating Conditions (MC) E2.A.13.1.3.1 and E2.A.13.1.3.2. apply to the facts of Applicant's case. However, since the misuse occurred at least four times in less than one calendar year, it was not an isolated event and MC E2.A13.1.3.4. is not applicable.

It is not clear that MC E2.A13.1.3.5. applies to Applicant's case, since his misuse was unintended and inadvertent and it would appear he was unaware of the misuse until confronted by his employer. Thus, a prompt, good faith effort to correct the situation was not possible. The record does not establish that Applicant's inadvertent misuse of his employer's technology system was the sole reason he was terminated from his job. I conclude that Applicant has mitigated the disqualifying conduct alleged in ¶¶ 1.a. and 1.b. of the SOR

Guideline E - Personal Conduct

In the SOR, DOHA alleged under Guideline E that Applicant misused his employer's information technology systems as alleged in ¶¶ 1.a. and 1.b and that the misuse reflected questionable judgment, untrustworthiness, unreliability, lack of candor, dishonesty or unwillingness to comply with rules and regulations and further suggested Applicant may not properly safeguard classified information (¶ 2.a.); that Applicant inaccurately dated a tank log prematurely in March 2002, which resulted in a letter of warning from his employer on March 25, 2002 (¶ 2.b.); and that he falsified material facts on his SF-86 when he denied, in answer to Question 22, that he had ever been fired from a job, quit a job after being told he'd be fired, left a job by mutual agreement following allegations of misconduct, left a job by mutual agreement following allegations of unsatisfactory performance, or left a job for other reasons under unfavorable circumstances (¶ 2.c.).

Guideline E conduct raises security concerns because it involves questionable judgment, untrustworthiness, unreliability, lack of candor, dishonesty, or unwillingness to comply with rules and regulations and could indicate that an applicant may not properly safeguard classified information. Directive ¶ E2.A5.1.l.

Applicant's conduct raises security concerns under four Disqualifying Conditions (DC) under Guideline E. First,

reliable, unfavorable information about Applicant's alleged unprofessional conduct and questionable judgment was provided by coworkers and associates, raising a concern under DC E2.A5.1.2.1 of the Guideline. Second, Applicant omitted relevant and material facts about his employment history in response to Question 22 on his SF-86, raising concern under DC E2.A5.1.2.2 of Guideline E. Third, Applicant's alleged personal conduct and concealment or misrepresentation of information increased his vulnerability to coercion, exploitation, or duress, raising a concern under DC E2.A5.1.2.4. Fourth, Applicant's alleged disqualifying personal conduct in falsely dating a tank log entry suggested a pattern of dishonesty or rule violations, raising a concern under DC E2.A5.1.2.5.

We turn to an examination of possible Mitigating Conditions (MC) under the Guideline. The information about Applicant's unprofessional conduct that was provided by Applicant's coworkers and associates at Company 1 was pertinent to a determination of his judgment, trustworthiness, or reliability. However, the information was provided to them by the Chief Engineer at Company 1 who was Applicant's supervisor, and Applicant supplied credible testimony supporting a conclusion that the Chief Engineer's allegations did not accurately or totally reflect what had actually happened. Therefore, MC E2.A5.1.3.1 is applicable. Additionally, MC E2.A5.1.3.3.applies in part to Applicant's case because he made a good-faith effort at the earliest opportunity in his interview with the DSS agent to set the record straight before being confronted with the facts. Applicant's conduct in carrying out his work as an employee of Company 2, as attested to in a letter dated October 18, 2004, from his current supervisor, indicates he had taken positive steps to significantly reduce or eliminate his vulnerability to coercion, exploitation, or duress, and thus MC E2.A5.1.3.5. is applicable. Accordingly, I find the Guideline E allegations of the SOR have been successfully mitigated by the Applicant.

In my evaluation of the record, I have carefully considered each piece of evidence in the context of the totality of evidence and under all the Directive guidelines that were generally applicable or might be applicable to the facts of this case. After weighing the facts of Applicant's case against the nine factors comprising the whole person concept, as specified at ¶ E2.2.of Enclosure 2 of the Directive, I conclude Applicant has successfully overcome the Government's case opposing his request for a DoD security clearance.[(4)]

FORMAL FINDINGS

The following are my conclusions as to the allegations in the SOR:

Paragraph 1.: Guideline M: FOR APPLICANT

Subparagraph 1.a.: For Applicant

Subparagraph 1.b.: For Applicant

Paragraph 2.: Guideline E: FOR APPLICANT

Subparagraph 2.a.: For Applicant

Subparagraph 2.b.: For Applicant

Subparagraph 2.c.: For Applicant

DECISION

In light of all of the circumstances presented by the record in this case, it is clearly consistent with the national interest to grant or continue a security clearance for Applicant. Clearance is granted.

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. The record shows that Company 1 stamped Applicant's Notice of Termination as "Processed" on April 11, 2001 (Ex. 4.) As an employee of Company 2, Applicant signed and dated his SF-86 on April 3, 2001 (Ex. 1.)

4. The nine factors comprising the whole person concept are as follows: the nature, extent, and seriousness of the conduct (E2.2.1.1); the circumstances surrounding the conduct, to include knowledgeable participation (E2.2.2.1.2.); the frequency and recency of the conduct (E2.2.1.3.); the individual's age and maturity at the time of the conduct (E2.2.1.4.); the voluntariness of participation (E2.2.1.5.); the presence or absence of rehabilitation and other pertinent behavioral changes (E2.2.1.6.); the motivation for the conduct (E2.2.1.7.); the potential for pressure, coercion, exploitation, or duress (E2.2.1.8); and the likelihood of continuation or recurrence (E2.2.1.9.).