KEYWORD: Personal Conduct; Criminal Conduct

DIGEST: Applicant was arrested for forgery, theft, and failure to appear in court. The charges were resolved under a pretrial diversion program. He did not disclose them on his security clearance application (SF 86) based on advice from his lawyer. His co-workers sent him sexually explicit e-mails. He did not initiate any of the e-mails or forward those he received, but he did not delete them from the temporary internet file folder on his government computer. He refuted the allegations of deliberately falsifying his SF 86 and mitigated the security concern based on his passive receipt of sexually explicit e-mails. Clearance is granted.

CASE NO: 05-00376.h1

DATE: 06/22/2006

DATE: June 22, 2006

In re:

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

Applicant for Security Clearance

ISCR Case No. 05-00376

DECISION OF ADMINISTRATIVE JUDGE

LEROY F. FOREMAN

APPEARANCES

FOR GOVERNMENT

Daniel F. Crowley, Esq., Department Counsel

FOR APPLICANT

Kevin L. Chapple, Esq.

SYNOPSIS

Applicant was arrested for forgery, theft, and failure to appear in court. The charges were resolved under a pretrial diversion program. He did not disclose them on his security clearance application (SF 86) based on advice from his lawyer. His co-workers sent him sexually explicit e-mails. He did not initiate any of the e-mails or forward those he received, but he did not delete them from the temporary internet file folder on his government computer. He refuted the allegations of deliberately falsifying his SF 86 and mitigated the security concern based on his passive receipt of sexually explicit e-mails. Clearance is granted.

STATEMENT OF THE CASE

On September 28, 2005, the Defense Office of Hearings and Appeals (DOHA) issued a Statement of Reasons (SOR) detailing the basis for its preliminary decision to deny Applicant a security clearance. The SOR alleges security concerns under Guidelines E (Personal Conduct) and J (Criminal Conduct). Under Guidelines E and J, it alleges Applicant falsified his SF 86 by intentionally failing to disclose two arrests (SOR ¶¶ 1.a.(1), 1.b.(1), 2.a). Under Guideline E, it alleges he accessed, received, and retained "sexually explicit images" on his government computer (¶¶ 1.c, 1.d).

Applicant answered the SOR in writing on October 19, 2005. DOHA returned his answer on October 27, 2005, because it was incomplete. He resubmitted his answer on November 8, 2005, admitting the facts alleged but denying intentional falsification of his SF 86 or any wrongdoing with his government computer. He requested a hearing. The case was assigned to me on February 8, 2006. On March 14, 2006, Applicant's lawyer entered his appearance. On March 16, 2006, DOHA issued a notice of hearing setting the case for April 20, 2006. The case was heard as scheduled. DOHA received the transcript (Tr.) on May 3, 2006.

FINDINGS OF FACT

Applicant's admissions in his answer to the SOR and at the hearing are incorporated into my findings of fact. I make the following findings:

Applicant is a 27-year-old employee of a federal contractor. While a college student, he worked in telemarketing for a major communications company and as a student intern for a federal office. He received a bachelor's degree in business administration in 2003 and has been employed by his current employer since July 2003. He was hired as a temporary contract employee for a government agency and three months later was promoted to be an accounts manager for the U.S. Department of State. Shortly thereafter, he was promoted to be an administrative assistant at the State Department. He received an interim clearance on July 29, 2003, but it was revoked on October 3, 2005.[(1)]

Applicant's resume lists technical proficiency in numerous software programs.[(2)] He testified he gained his proficiency during his employment at the State Department.[(3)] His immediate supervisor considered him "extremely professional and diligent," with a "very positive attitude" and good technical computer skills.[(4)] A principal deputy director stated Applicant showed "admirable willingness to learn new skills, computer applications and office procedures."[(5)] His supervisor in the grants management office at his first place of duty found him to be highly motivated with a "great work ethic." She regarded him as a self-starter and a team player.[(6)] His supervisor in the human resources office found him charming, friendly, sophisticated, mature, and totally trustworthy.[(7)]

Applicant executed an SF 86 on July 25, 2003. He answered "no" to question 21, asking if he had ever been charged with or convicted of any felony offense. He also answered "no" to question 26, asking if he had been arrested, charged with, or convicted of any offenses not listed elsewhere.[(8)] He did not disclose his arrest on October 9, 2000, for forgery (a felony) and theft by conversion; and his arrest on August 28, 2002, for failing to appear at a hearing on the forgery and theft offenses.

The charges of forgery and theft arose while Applicant was a college student. He allowed several fellow students to use his campus mail box because there were not enough mail boxes for all students. Students who worked in the mail room also had access to his mail box. The forgery and theft charges were based on misuse of credit card applications sent to Applicant's mail box. He denied being involved in credit card fraud.

Applicant's lawyer, a public defender, advised him he was facing five years in prison, but that if he performed community service the case would be on a "dead docket like it never, ever happened." He asked his lawyer whether he should disclose his arrest on future job applications, and she advised not to disclose it, because it would be "washed

away." [(9)]

Applicant's hearing on the forgery and theft charges was scheduled to occur while he was away on summer break. On August 28, 2002, he returned to college and was arrested for failure to appear in court. On September 5, 2002, all the offenses were placed on the "dead docket" pending completion of pretrial intervention.[(10)] He was ordered to perform three months of community service, which he completed. At the hearing, he denied knowing he had a felony arrest.[(11)]

On August 8, 2004, computer security investigators found "sexually explicit inappropriate" images in the temporary internet files folder on Applicant's government computer. The images were not included or described in the investigative file, except for one attachment to an e-mail that was described by the investigators as portraying bestiality between a man and a horse.[(12)] Applicant testified the investigators also showed him an image of the backside of a very large woman.[(13)]

Applicant was interviewed by the computer security investigators on November 5, 2004. He explained that the materials were sent to him by friends and he did not forward the materials to anyone. He did not think the presence of the materials was "a problem" because he was the recipient, not the sender. According to the investigators, he apologized for his conduct, and the interview "terminated under favorable circumstances."[(14)]

At the hearing, Applicant testified that he never saw the image portraying bestiality because the investigators were unable to open the file on his computer.[(15)] He testified the e-mail attachments were pictures of beach parties and personal photographs, but he insisted none of them showed nudity or sexual acts.[(16)] He thought the e-mails were "inappropriate" because he believed personal e-mail should not be sent or viewed at work.[(17)]

Applicant was one of the youngest workers in the office. He was not concerned when he received the e-mails, because all the e-mails were from co-workers, and they were regarded as jokes.[(18)]

Applicant testified he was familiar with using the computer for accounting, but he knew little about e-mail files. He had little experience with e-mail in college and previous jobs. He first used e-mail regularly at the State Department.[(19)] He testified he does not know what a temporary internet file folder is and does not know how to delete e-mails or images from it.[(20)]

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 authorized the Secretary of Defense or his designee to grant applicants eligibility for access to classified information "only upon a finding that it is clearly consistent with the national interest to do so." Exec. Or. 10865, *Safeguarding Classified Information within Industry* § 2 (Feb. 20, 1960), as amended and modified. Eligibility for a security clearance is predicated upon the applicant meeting the security guidelines contained in the Directive. 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 (App. Bd. Dec. 19, 2002).

The Directive sets forth adjudicative guidelines for determining eligibility for access to classified information, and it lists the disqualifying conditions (DC) and mitigating conditions (MC) for each guideline. Each clearance decision must be a fair, impartial, and commonsense decision based on the relevant and material facts and circumstances, the whole person concept, and the factors listed in the Directive ¶¶ 6.3.1. through 6.3.6.

In evaluating an applicant's conduct, an administrative judge should consider: (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 applicant's age and maturity at the time of the conduct; (5) the voluntariness of participation; (6) the presence or absence of rehabilitation and other pertinent 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. Directive ¶¶ E2.2.1.1. through E2.2.1.9.

A person granted access to classified information enters into a special relationship with the government. The government must be able to have a high degree of trust and confidence in persons with access to classified information. However, 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 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 which disqualify, or may disqualify, the applicant from being eligible for access to classified information. *See Egan*, 484 U.S. at 531. "[T]he Directive presumes there is a nexus or rational connection between proven conduct under any of the Criteria listed therein and an applicant's security suitability." ISCR Case No. 95-0611 at 2 (App. Bd. May 2, 1996) (quoting DISCR Case No. 92-1106 (App. Bd. Oct. 7, 1993)).

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; *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 (App. Bd. Dec. 19, 2002). "[S]ecurity clearance determinations should err, if they must, on the side of denials." *Egan*, 484 U.S. at 531; *see* Directive ¶ E2.2.2.

CONCLUSIONS

Guideline E (Personal Conduct-Falsification of the SF 86)

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. A disqualifying condition (DC 2) under this guideline may be established by "deliberate omission, concealment, or falsification of relevant and material facts from any personnel security questionnaire, personal history statement, or similar form used to conduct investigations, determine employment qualifications, award benefits or status, determine security clearance eligibility or trustworthiness, or award fiduciary responsibilities." Directive ¶ E2.A5.1.2.2.

Where, as in this case, a falsification allegation is controverted, the government has the burden of proving it. Proof of an omission, standing alone, does not establish or prove an applicant's state of mind when the omission occurred. An administrative judge must consider the record evidence as a whole to determine whether there is direct or circumstantial evidence concerning an applicant's state of mind at the time the omission occurred. *See* ISCR Case No. 03-09483 at 4 (App. Bd. Nov. 17, 2004).

Applicant did not know he had been charged with a felony. His lawyer told him that if he completed the pretrial diversion his record would be clean. He specifically asked his lawyer about disclosing his arrests on employment applications and was advised there would be nothing to disclose. I found Applicant's explanations plausible. After hearing his testimony, observing his demeanor, and considering all the evidence, I found him credible. I am satisfied he did not intentionally falsify his answers to questions 21 and 26. Accordingly, I resolve SOR ¶¶ 1.a.(1) and 1.b.(1) in his favor.

Guideline E (Personal Conduct-Sexually Explicit E-mails)

A disqualifying condition (DC 1) may arise from "[r]eliable, unfavorable information provided by associates, employers, coworkers, neighbors, and other associates." A disqualifying condition (DC 4) also may arise from "[p]ersonal conduct . . . that increases an individual's vulnerability to coercion, exploitation, or duress, such as engaging in activities which, if known, may affect the person's personal, professional, or community standing or render the person susceptible to blackmail." Directive ¶ E2.A5.1.2.4. The computer security investigators at Applicant's workplace provided "reliable, unfavorable information" sufficient to establish DC 1. The presence of at least one vulgar, sexually explicit image on Applicant's government computer was sufficient to establish DC 4.

A security concern under this guideline can be mitigated (MC 5) by evidence of "positive steps to significantly reduce or eliminate vulnerability to coercion, exploitation, or duress." Directive ¶ E2.A5.1.3.5. After being interviewed by computer security investigators, Applicant apologized and promised to be more vigilant in his use of government computers in the future. His contrite response and his forthright disclosure of the facts eliminated his vulnerability to coercion, exploitation, or duress. I conclude MC 5 is established.

Several factors under the general adjudicative guidelines are relevant. The extent to which sexually explicit e-mails were involved is difficult to determine in light of the sparse evidence. Only one sexually explicit e-mail is specifically identified in the investigative report, and Applicant voluntarily described a second e-mail that was gross and vulgar, but not necessarily sexual. Applicant denied seeing any sexually explicit e-mails on his computer. *See* Directive ¶ E2.2.1.1 (nature, extent, and seriousness of conduct).

The e-mails were instigated by Applicant's co-workers. He did not actively seek sexually explicit materials, nor did he forward any e-mails from his co-workers. He regarded the e-mails as jokes. His involvement was purely passive. *See* Directive ¶ E2.2.1.2 (circumstances surrounding the conduct).

The time frame of the conduct ended in August 2004. The investigative file does not indicate the dates or frequency of the inappropriate e-mails. The evidence establishes one sexually explicit image and one vulgar but not necessarily sexual image. *See* Directive ¶ E2.2.1.3 (frequency and recency of conduct). Applicant was the youngest member of his work group, a recent college graduate, and relatively new to government service. *See* Directive ¶ E2.2.1.4 (age and maturity). The investigation was a wake-up call for Applicant. He cooperated with investigators and was contrite. He is well regarded by his supervisors. He impressed me at the hearing as somewhat naive but sincere and honest. I conclude the likelihood of recurrence is nil. *See* Directive ¶¶ E2.2.1.6 (rehabilitation) and E2.2.1.9 (likelihood of recurrence).

After weighing the disqualifying and mitigating conditions and evaluating the evidence in the context of the whole person, I conclude Applicant has mitigated the security concern arising from his involvement in inappropriate e-mails. Thus, I resolve SOR ¶¶ 1.c and 1.d in his favor.

Guideline J (Criminal Conduct)

Under this guideline, a single serious offense can raise a security concern (DC 2). It is a felony, punishable by a fine or imprisonment for not more than five years, or both, to knowingly and willfully make any materially false, fictitious, or fraudulent statement or representation in any matter within the jurisdiction of the executive branch of the Government of the United States. 18 U.S.C. § 1001. Security clearances are within the jurisdiction of the executive branch of the Government of the United States. *See Egan*, 484 U.S. at 527. A deliberately false answer on a security clearance application is a serious crime within the meaning of Guideline J. For the reasons discussed above, I am satisfied Applicant did not intentionally falsify his SF 86 and did not violate 18 U.S.C. § 1001. Accordingly, I resolve SOR ¶ 2.a. in his favor.

FORMAL FINDINGS

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

Paragraph 1. Guideline E (Personal Conduct): FOR APPLICANT

Subparagraph 1.a.(1): For Applicant

Subparagraph 1.b.(1): For Applicant

Subparagraph 1.c.: For Applicant

Subparagraph 1.d.: For Applicant

Paragraph 2. Guideline J (Criminal Conduct): FOR APPLICANT

Subparagraph 2.a.: For Applicant

DECISION

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

LeRoy F. Foreman

Administrative Judge

1. Tr. 46-47.

2. Applicant's Exhibit (AX) A.

3. Tr. 64.

4. AX B.

5. AX C.

6. AX D.

7. AX E.

8. Government Exhibit (GX) 1 at 5.

9. Tr. 52-56.

10. GX 2; GX 3.

11. Tr. 76.

12. GX 5 at 3.

13. Tr. 79.

14. GX 5 at 5.

15. Tr. 58.

16. Tr. 78.

17. Tr. 58-59.

18. Tr. 79-80.

19. Tr. 66-67.

20. Tr. 60.