KEYWORD: Criminal Conduct; Information Technology; Personal Conduct; Financial

DIGEST: Applicant stole $40,000.00 from a deceased mutual fund owner's account by using his employer's information technology system and was fired from two jobs for absenteeism and failure to follow rules. He disclosed only one firing on his security clearance application (SF 86). Security concerns arising from his employment record are mitigated, but concerns based on the theft and falsification of his SF 86 are not mitigated. Clearance is denied.

CASENO: 03-15336.h1

DATE: 01/27/2005

DATE: January 27, 2005

In Re:

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

Applicant for Security Clearance

ISCR Case No. 03-15336

DECISION OF ADMINISTRATIVE JUDGE

LEROY F. FOREMAN

APPEARANCES

FOR GOVERNMENT

Kathryn Antigone Trowbridge, Esq., Department Counsel

FOR APPLICANT

Jason C. Mills, Esq.

SYNOPSIS

Applicant stole $40,000.00 from a deceased mutual fund owner's account by using his employer's information technology system and was fired from two jobs for absenteeism and failure to follow rules. He disclosed only one firing on his security clearance application (SF 86). Security concerns arising from his employment record are mitigated, but concerns based on the theft and falsification of his SF 86 are not mitigated. Clearance is denied.

STATEMENT OF THE CASE

On March 18, 2004, the Defense Office of Hearings and Appeals (DOHA) issued a Statement of Reasons (SOR) detailing the basis for its decision to deny Applicant a security clearance. This action was taken under Executive Order 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). The SOR alleges security concerns under Guidelines J (Criminal Conduct), E (Personal Conduct), M (Misuse of Information Technology Systems), and F (Financial Considerations). Under Guidelines J, E, M, and F, the SOR alleges Applicant, while employed by a large investment company, transferred $40,000.00 from a deceased client's mutual fund account to his own personal checking account. Under Guideline E, the SOR alleges Applicant was fired from two jobs and falsified his security clearance application by disclosing only one of the two firings.

Applicant answered the SOR in writing on March 26, 2004, admitted all the allegations except falsifying his security clearance application, and requested a hearing. The case was initially assigned to another administrative judge but reassigned to me on September 23, 2004. DOHA issued a notice of hearing on the same day, setting the case for October 21, 2004. The case was heard as scheduled. DOHA received the transcript (Tr.) on October 29, 2004.

FINDINGS OF FACT

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

Applicant is a 30-year-old structural analyst for a defense contractor. He has worked for his current employer for about three and a half years. He does not have a security clearance.

Applicant graduated from college in June 1997with a degree in applied physics. He received a master's degree in aerospace in engineering in 2001. He is currently pursuing another master's degree in technical management and business administration.

In October 1997, when he was 22 years old, he began working for an investment company as an account representative. On February 4, 1998, in the normal course of his duties, he accessed the company's information system and noticed a mutual fund account of a deceased client. He electronically transferred $40,000.00 from the deceased client's account to his own personal checking account. He changed some of the identifying data to delay the confirmation statements pertaining to the transaction. After making the transfer, Applicant was absent from work until February 16, 1998, without authorization or notice to his supervisor. Applicant testified this absence was due to illness. When he returned, he was fired for his unauthorized absence. The company was not yet aware of the illegal transfer of funds.

On February 17, 1998, the day after Applicant was fired, the company received an incoming wire for $40,000.00, listing Applicant as the originator. The wire could not be processed because it was not formatted accurately, and it was returned to the originating bank.

On March 10, 1998, a representative of the deceased client informed the company the documentation had been completed to transfer about $40,000.00 into a trust account, and the company responded that the money had been transferred out of the account. At this point, the company became aware of the illegal transfer of funds. On March 16, 1998, Applicant's bank returned the $40,000.00 to Applicant's former employer. There is no evidence Applicant used any of the money. Applicant knew returning the money was likely to identify him as the perpetrator.

Applicant was interviewed by the police on March 23, 1998, and he admitted transferring the funds to his own account. Applicant asserted he was "just fooling around" on his computer, did not expect the transaction to be accomplished, and never intended to keep the money.

Applicant was arrested and charged with a computer crime and grand theft, both felonies. With the consent of the company, Applicant entered a pretrial intervention program (PTIP), requiring him to pay a fine and perform 200 hours of community service. The record does not reflect whether the family and heirs of the deceased account holder agreed to the PTIP. Applicant completed the terms of the PTIP in March 2000, and the charges were dismissed.

While Applicant was in college, he accumulated considerable credit card debt. In May 2003, he told a Defense Security Service (DSS) investigator he "let the balances [on his credit card account] get out of control" while he was in college. He also told the investigator he "could not afford to pay the debt [he] accumulated on these credit cards" after he graduated. (Government Exhibit 2, pp. 2-3) At the hearing he testified he did not need money when he was working at the company because he was living with his parents and they "were also there to help [him] financially." (Tr. 60, 75)

Applicant testified he had been accepted at the United States Air Force Officers' Training School before his illegal transfer of funds caused that opportunity to be withdrawn. He testified he was remorseful for his conduct because of the sin he had committed and the shame it brought to his family, friends, and himself. (Tr. 30) He referred to the incident as a "most egregious and most horrific event," an "egregious lapse in judgment" and "pure stupidity." (Tr. 29) He was extremely emotional during his testimony, and it was necessary to recess the hearing once when he lost his composure. (Tr. 22)

In September 2000, while Applicant was a graduate student, he started working for a manufacturing engineering company through a student cooperative program. In February 2001, he was terminated from this job for unauthorized absences, using the company computer to manage personal business on company time, and making long personal calls on company time. His supervisor stated Applicant "could not, or did not work on his own" and "needed to be supervised at all times." (Government Exhibit 4) His supervisor said he was fired; Applicant testified he resigned by mutual agreement.

In July 2001, Applicant executed a security clearance application (SF 86). He disclosed he had been charged with "theft," but he did not list the computer crime charge. He stated the theft charges were dismissed, but he did not mention the PTIP. He disclosed he left the manufacturing design company in February 2001 "by mutual agreement following allegations of unsatisfactory performance." Applicant did not disclose his termination by the investment company in 1998 for unauthorized absence.

At the hearing, Applicant testified he did not mention his termination by the investment company because he made a "mistaken assumption" that it would be revealed in the investigation of the theft, since he told the police he had been fired for his unauthorized absence. (Tr. 39) He also testified he thought the police report would reveal his successful completion of the PTIP as the basis for dismissing the charges. He denied intending to falsify his security clearance application.

At the hearing, Applicant submitted several statements attesting to his good character. Applicant's current supervisor regards him as having "a high degree of integrity, responsibility, and ambition," exhibiting "good judgment and mature outlook." A colleague regards him as "a conscientious worker, a kind and sincere individual, and an ideal coworker." A member of Applicant's church considers Applicant as exhibiting "a high degree of trustworthiness and loyalty to his work," with "a strong spiritual background which affects his morals and ethics in a very positive way." An elder of Applicant's church considers him "a person of excellent moral character and integrity." His supervisor and two church members were aware of Applicant's illegal transfer of mutual funds. (Tr. 55)

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.

The Directive sets out the adjudicative guidelines for making decisions on security clearances. Enclosure 2 of 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.

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, that conditions exist 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 (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 (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

Guidelines J, M, and F (Illegal Transfer of Funds)

Under Guideline J, a serious crime can raise a security concern and be disqualifying. Directive ¶ E2.A10.1.2. Under Guideline M, illegal or unauthorized manipulation of information residing on an information technology system is a disqualifying condition. Directive ¶ E2.A13.1.2.2. Under Guideline F, embezzlement, employee theft, and other intentional financial breaches of trust are disqualifying. Directive ¶ E2.A6.1.2.2. Applicant's admission he manipulated his employer's information system to transfer $40,000.00 from a client's account to his own establishes disqualifying conditions under Guidelines J, M, and F.

The security concerns raised by a serious crime can be mitigated by showing it was not recent, an isolated incident, or "clear evidence" of successful rehabilitation. Directive ¶¶ E2.A10.1.3.1., E2.A10.1.3.2., E2.A10.1.3.6. Similarly, misuse of an information technology system can be mitigated by showing the misuse was not recent or an isolated event. Directive ¶¶ E2.A13.1.3.1., E2.A13.1.3.4. Finally, intentional financial breaches of trust under Guideline F can be mitigated by showing the behavior was not recent or was an isolated incident. Directive ¶¶ E2.A6.1.3.1., E2.A6.1.3.2.

There are no "bright line" rules for determining when conduct is "recent." The determination must be based "on a careful evaluation of the totality of the record within the parameters set by the directive." ISCR Case No. 02-24452 at 6 (App. Bd. Aug. 4, 2004). If the evidence shows "a significant period of time has passed without any evidence of misconduct," then the Administrative Judge must determine whether that period of time demonstrates "changed

circumstances or conduct sufficient to warrant a finding of reform or rehabilitation." *Id*. Whether criminal conduct is "recent" or "isolated" is related to the question of rehabilitation. The decisional issues are whether there has been a significant period of time without any evidence of misconduct, and whether the evidence shows changed circumstances or conduct.

Applicant's theft was not an isolated event. It was the most serious in a series of irresponsible acts. His theft was followed by termination for unauthorized absence and termination from another job three years later for unsatisfactory performance, absenteeism, and misuse of company facilities for personal business.

I am not satisfied sufficient time has passed to mitigate the theft, nor am I satisfied there is "clear evidence" of rehabilitation. Applicant's testimony and demeanor clearly reflect his belief the theft of the $40,000.00 was morally wrong, and he is profoundly embarrassed by it. I cannot determine from the record whether Applicant returned the money because of remorse, fear, or both. I also cannot determine whether Applicant's present attitude is remorse, embarrassment, or both. I have concerns based on Applicant's testimony at the hearing, which indicates a tendency to minimize and rationalize unfavorable information. He persisted in his original explanation that he was "just fooling around" when he transferred the money. He had no explanation for choosing to "fool around" with $40,000.00 instead of an inconsequential amount. His elaborate measures to delay the confirmation statement and thereby delay detection of the fraud are not consistent with "just fooling around." To the contrary, they suggest a premeditated theft.

Furthermore, Applicant's testimony at the hearing about his financial situation at the time of the theft concerns me. He disclosed two delinquent credit card accounts on his SF 86. In May 2003, he told a DSS investigator the accounts were "out of control" and he could not afford to pay the debts. However, at the hearing, when it was obvious that his credit card debt was a possible motive for the theft, Applicant testified he did not need money at the time of the theft because he was living with his parents and they were available to help him financially.

Applicant's tendency to minimize unfavorable information is also reflected in his omission of the fact that he was fired by the investment company in February 1998, and in his description of his termination of employment in February 2001. Applicant insisted at the hearing his termination in February 2001 was by mutual agreement. The evidence from his supervisor unequivocally stated Applicant was fired.

Applicant has the burden of establishing mitigating conditions as well as the burden of persuasion on the ultimate question whether he should receive a security clearance. Directive ¶ E3.1.15. I am concerned about his apparent lack of candor. Because of his tendency to minimize and rationalize, I am not satisfied he would report a security violation committed by himself or others if it would be personally embarrassing or professionally detrimental. He has failed to persuade me there is "clear evidence" of rehabilitation. I conclude the security concerns under Guidelines J, M, and F are not mitigated.

Guideline E (Personal Conduct)

Conduct involving questionable judgment, untrustworthiness, unreliability, lack of candor, dishonesty, or unwillingness to comply with rules and regulations could indicate the applicant may not properly safeguard classified information. Directive ¶ E2.A5.1.1. A disqualifying condition under this guideline can be raised by reliable unfavorable information from employers (DC 1). Directive ¶ E2.A5.1.2.1. Applicant's theft of $40,000.00 demonstrates questionable judgment and dishonesty. He was fired from two jobs for unreliability and unwillingness to comply with rules. I conclude DC 1 is established.

None of the mitigating conditions enumerated in the Directive are applicable. Based on the general adjudicative guidelines, however, I conclude the security concerns raised by applicant being twice fired for unreliability and unwillingness to comply with rules are mitigated by the passage of time without similar conduct and his performance in his current job. *See* Directive ¶¶ 6.3.2. (recency of conduct), 6.3.5. (rehabilitation), 6.3.6. (probability of recurrence). His theft of $40,000.00 is not mitigated, however, for the reasons set out in the discussion of Guidelines J, M, and F, above.

The deliberate omission of relevant and material facts from a security questionnaire is a disqualifying condition (DC 2) that can raise a security concern. When a falsification allegation is controverted, Department Counsel has the burden of proving it. Proof of an omission, standing alone, does not establish or prove an applicant's intent or 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 intent or state of mind at the time the omission occurred. ISCR Case No. 03-09483 at 4 (App. Bd. Nov. 17, 2004).

Applicant admitted omitting his termination by the investment company for unauthorized absence. He has denied intending to falsify his application, explaining he thought the information about the firing would be included in the police records regarding the theft. The police records reflect Applicant's admission he was fired for unauthorized absence.

Based on this record, I am satisfied Applicant's embarrassment and tendency to minimize adverse information motivated him to omit the information, and he justified the omission in his mind by concluding the firing would be reflected in the police report of the theft. I find his explanation for the omission disingenuous at best. I conclude the omission was intentional.

A falsification can be mitigated by a prompt, good-faith effort to correct it before being confronted with the facts. Directive ¶ E2.A5.1.3.3. Applicant executed his SF 86 in July 2001, but he did not correct the omission until he was questioned about it by a DSS investigator in May 2003. The security concerns raised by Applicant's falsification are not mitigated.

FORMAL FINDINGS

Paragraph 1. Guideline J (Criminal Conduct): AGAINST APPLICANT

Subparagraph 1.a.: Against Applicant

Paragraph 2. Guideline E (Personal Conduct): AGAINST APPLICANT

Subparagraph 2.a.: Against Applicant

Subparagraph 2.b.: For Applicant

Subparagraph 2.c.: For Applicant

Subparagraph 2.d.: Against Applicant

Paragraph 3. Guideline M (Information Technology): AGAINST APPLICANT

Subparagraph 3.a.: Against Applicant

Paragraph 4. Guideline F (Financial Considerations): AGAINST APPLICANT

Subparagraph 3.a.: Against Applicant

DECISION

In light of all the circumstances presented by the record in this case, it is not clearly consistent with the national interest to grant a security clearance for Applicant. Clearance is denied.

LeRoy F. Foreman

Administrative Judge