KEYWORD: Personal Conduct; Criminal Conduct

DIGEST: Applicant falsely stated in writing and under oath that he had never engaged in misuse of information technology systems. He later admitted computer hacking while in college. The security concern based on his false sworn statement is not mitigated. Clearance is denied.

CASENO: 04-11704.h1

DATE: 02/13/2006

DATE: February 13, 2006

In re:

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

Applicant for Security Clearance

ISCR Case No. 04-11704

DECISION OF ADMINISTRATIVE JUDGE

LEROY F. FOREMAN

APPEARANCES

FOR GOVERNMENT

Jason Perry, Esq., Department Counsel

FOR APPLICANT

Pro Se

SYNOPSIS

Applicant falsely stated in writing and under oath that he had never engaged in misuse of information technology systems. He later admitted computer hacking while in college. The security concern based on his false sworn statement is not mitigated. Clearance is denied.

STATEMENT OF THE CASE

On July 19, 2005, the Defense Office of Hearings and Appeals (DOHA) issued a Statement of Reasons (SOR) detailing the basis for its preliminary decision to not grant a security clearance to Applicant. 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 Guideline E (Personal Conduct) and J (Criminal Conduct). The concern under both guidelines was based on falsification of material facts during a security interview. Applicant answered the SOR in writing on July 28, 2005, denied intentional falsification, and elected to have the case decided on the written record in lieu of a hearing. Department Counsel submitted the Government's written case on November 17, 2005. A complete copy of the file of relevant material (FORM) was provided to Applicant, and he was afforded an opportunity to file objections and submit material to refute, extenuate, or mitigate the disqualifying conditions. Applicant received the FORM on November 23, 2005, and he did not submit any additional material. The case was assigned to me on January 23, 2006.

FINDINGS OF FACT

Based on the entire record, including Applicant's admissions in his response to the SOR, I make the following findings of fact:

Applicant is a 28-year-old software developer for a federal contractor. He graduated from college in December 1999 and was unemployed until February 2000, when he began working for a federal contractor in a computer support position. He applied for a security clearance in March 2000, but his application was denied in December 2001.[(1)] He began working for his current employer in September 2002.

In preparation for his current position, he executed a SF 86 on August 28, 2002. He was interviewed by a security investigator on April 12, 2004, and he executed a signed, sworn statement asserting he had never engaged in misuse of information technology systems, to include hacking, pirating, illegal or unauthorized downloads.[(2)] In a second security interview on September 21, 2004, he admitted using a port scanner, "a sort of hacking device," while in college in 1999. He used it to download MP3 files from the internet, connect to other individuals' computers, search for shared files, and access those of interest to him. He did not know if the MP3 files were pirated, but he recognized the possibility they were.[(3)] In his answer to the SOR, Applicant repeated his admission of misusing information technology systems, but insisted it "slipped his mind" during the first security interview.[(4)]

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.

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)

Under this guideline, conduct involving questionable judgment, untrustworthiness, unreliability, lack of candor, dishonesty, or unwillingness to comply with rules and regulations could indicate that the person may not properly safeguard classified information. Directive ¶ E2.A5.l.l. A disqualifying condition (DC 3) may apply when an applicant deliberately provides false or misleading information concerning relevant and material matters to an investigator or security official in connection with a personnel security or trustworthiness determination. Directive ¶E2.A5.11.2.3.

When 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 of the omission. *See* ISCR Case No. 03-09483 at 4 (App. Bd. Nov. 17, 2004).

Applicant admits his statement of August 28, 2002 was false, but claims his computer hacking in 1999 "slipped his mind." I find his explanation implausible and unconvincing. He is a well-educated, mature adult. He previously had submitted a security application and had been rejected. He knew his first application had been subjected to close scrutiny. He made a written, detailed, specific, categorical denial of computer hacking, and swore to it. The hacking was not in his distant past, but occurred no more than three years before he executed his sworn statement. His hacking was not a single, isolated, event, but a course of conduct involving a variety of activities. It is implausible that his detailed, sworn denial of hacking did not trigger memory of his hacking activities in college. I conclude DC 3 is established.

Two mitigating conditions (MC) are relevant to this case. MC 2 applies when the falsification was an isolated incident, was not recent, and the individual has subsequently provided correct information voluntarily. Directive ¶ E2.A5.1.3.2. MC 3 applies when the individual made prompt, good-faith efforts to correct the falsification before being confronted with the facts. Directive ¶ E2.A5.1.3.3.

Applicant has the burden of proving a mitigating condition, and the burden of disproving it is never shifted to the government. *See* ISCR Case No. 02-31154 at 5 (App. Bd. Sep. 22, 2005). I conclude Applicant has not carried his burden of establishing MC 2 or MC 3. Applicant's falsification was "recent," because it occurred during his current security investigation. He did not voluntarily provide the correct information. He admitted his computer hacking only after he was questioned a second time by a security investigator.

In addition to the enumerated disqualifying and mitigating conditions under this guideline, I have also considered the seriousness of Applicant's conduct, his age and maturity at the time of his falsification, and the fact this case involves a single act of falsification rather than a course of conduct. *See* Directive ¶¶ E2.2.1.1. (nature, extent, and seriousness of conduct), E2.2.1.4. (age and maturity), E2.2.1.3. (frequency and recency of conduct). His conduct is serious, as noted below under Guideline J. His history of computer hacking especially was especially significant in assessing his suitability for a clearance, in light of his sensitive position as a software developer. He is a well-educated, mature adult who should have understood the seriousness of providing false information during a security investigation. On the other hand, a single falsification is less serious than a pattern of falsification, and the absence of repeated falsification is a somewhat mitigating condition.

After weighing the disqualifying and mitigating conditions and evaluating all the evidence in the context of the whole person, I conclude Applicant has not mitigated the security concern based on his false statement to a security investigator.

Guideline J (Criminal Conduct)

A history or pattern of criminal activity creates doubt about an applicant's judgment, reliability, and trustworthiness. Directive ¶ E2.A10.1.1. A disqualifying condition may be based on allegations or an applicant's admission of criminal conduct, whether or not charged (DC 1). Directive ¶ E2.A10.1.2.1. A single serious crime or multiple lesser offenses may be disqualifying (DC 2). Directive ¶ E2.A10.1.2.2.

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 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 in a security interview is a serious crime within the meaning of Guideline J. For the reasons discussed above under Guideline E, I conclude Applicant has not refuted the allegation of falsification. Accordingly, I conclude DC 1 and DC 2 under this guideline are established.

Criminal conduct can be mitigated by showing it was not recent (MC 1) or there is evidence of successful rehabilitation (MC 6). Directive ¶¶ E2.A10.1.3.1., E2.A10.1.3.6. The issues under both MC 1 and MC 6 are whether there has been a significant period of time without any evidence of misconduct, and whether the evidence shows changed circumstances or conduct. "Only with the passage of time will there be a track record that shows whether a person, through actions and conduct, is willing and able to adhere to a stated intention to refrain from acting in a way that the person has acted in the past." ISCR Case No. 97-0727, 1998 DOHA LEXIS 302 at *7 (App. Bd. Aug. 3, 1998).

The Directive is silent on what constitutes a sufficient period of reform and rehabilitation. The sufficiency of an applicant's period of conduct without recurrence of past misconduct does not turn on any bright-line rules concerning the length of time needed to demonstrate reform and rehabilitation, but rather on a reasoned analysis of the facts and circumstances of an applicant's case. If the record evidence shows a significant period of time has passed without evidence of misconduct, then an administrative judge must articulate a rational basis for concluding why that significant period of time does not demonstrate changed circumstances or conduct sufficient to warrant a finding of reform or rehabilitation. ISCR Case No. 02-24452 at 6 (App. Bd. Aug. 4, 2004).

Applicant has never held a security clearance, and his false statement occurred early in his career as a federal contractor. He does not yet have a sufficient track record of trustworthiness to demonstrate rehabilitation or a low likelihood of recurring falsification. I conclude he has not established MC 1 and MC 6.

A security concern based on criminal conduct also may be mitigated by showing the criminal behavior was "an isolated incident" (MC 2). Directive ¶E2.A10.1.3.2.; *see also* Directive, ¶ E2.2.1.3. (frequency and recency of conduct). There is no other evidence of falsification in this record. I conclude MC 2 is established.

After weighing the disqualifying and mitigating conditions and evaluating the evidence in the context of the whole person, I conclude Applicant has not mitigated the security concern based on his criminal conduct.

FORMAL FINDINGS

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

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

Subparagraph 1.a.: Against Applicant

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

Subparagraph 2.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 Applicant a security clearance. Clearance is denied.

LeRoy F. Foreman

Administrative Judge

1. FORM Item 4 at 9.

2. FORM Item 5 at 2.

3. FORM Item 6 at 1.

4. FORM Item 3.