KEYWORD: Sexual Behavior; Personal Conduct; Information Technology

DIGEST: Applicant accessed numerous pornographic web sites on a computer owned by his government contractor employer during a five-day period in January 2001. He also failed to fill out his time card on a daily basis as required by government regulations during that same time period. He has mitigated the security concerns caused by his conduct. Clearance is granted.

CASENO: 03-00987.h1

DATE: 09/17/2004

DATE: September 17, 2004

In Re:

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

Applicant for Security Clearance

ISCR Case No. 03-00987

DECISION OF ADMINISTRATIVE JUDGE

HENRY LAZZARO

APPEARANCES

FOR GOVERNMENT

Juan J. Rivera, Esq., Department Counsel

FOR APPLICANT

Gary L. Rigney, Esq.

SYNOPSIS

Applicant accessed numerous pornographic web sites on a computer owned by his government contractor employer during a five-day period in January 2001. He also failed to fill out his time card on a daily basis as required by government regulations during that same time period. He has mitigated the security concerns caused by his conduct. Clearance is granted.

STATEMENT OF THE CASE

On December 8, 2003, the Defense Office of Hearings and Appeals (DOHA) issued a Statement of Reasons (SOR) to Applicant stating they were unable to find it is clearly consistent with the national interest to grant or continue a security clearance for Applicant.[(1)] The SOR, which is in essence the administrative complaint, alleges security concerns under Guideline M (misuse of information technology systems), Guideline E (personal conduct), and Guideline D (sexual behavior) based upon Applicant's conduct in accessing pornographic web sites on his employer's computer and failing to fill out his time card on a daily basis as required by government regulations. Applicant submitted an answer to the SOR on January 6, 2004, denied the allegations contained in the SOR, and requested a hearing.

The case was assigned to me on May 24, 2004. A notice of hearing was issued on June 7, 2004, scheduling the hearing for June 15, 2004.[(2)] The hearing was conducted as scheduled. The government called the Applicant to testify in its case-in-chief, presented one other witness, and submitted 12 documentary exhibits that were marked as Government Exhibits (GE) 1-12, and admitted into the record without an objection. The Applicant testified, called five witnesses to testify on his behalf, and submitted one documentary exhibit that was marked as Applicant Exhibit (AE) 1, and admitted into the record without an objection. The transcript was received July13, 2004.

FINDINGS OF FACT

After a thorough review of the pleadings, exhibits and testimony, I make the following findings of fact:

Applicant is a 41-year-old man who has been married since August 1990. He obtained a bachelor of science degree in May 1989, and has worked for various federal contractors as either an engineer or systems analyst since November 1991. He has worked as an engineer for his present employer, a defense contractor, since July 1997. He has possessed a secret security clearance since March 1992. He self-reported a security violation he committed in October 2002 based upon his forgetting to enable a motion sensor while charged with the responsibility of closing up a secure facility at the end of the work day. No actual compromise of classified information occurred as a result of this incident because of the redundant security systems in place.

Applicant presented the testimony of several character witnesses, including the founder and CEO, the president, the vice president, and the manager of his present employer. They have each worked closely with him for as much as 12 years, and each have sound foundations for the opinions they expressed. Collectively, they established that Applicant is a good and respected employee who has a reputation of being honest, dedicated, and conscientious. They were each aware of the reasons for the hearing, but still expressed their opinion that Applicant is a man who follows rules and regulations.

At the time of the incidents in question, Applicant was working under a government contract at a facility owned by a contractor other than his employer. While working at the other facility, Applicant was provided with a computer by his employer that was installed in the other facility and routed through the other contractor's server.

Applicant accessed pornographic web sites on numerous occasions on January 15, 16, 18, and 19, 2001. His access of those sites was detected by a security system on or about January 25, 2001, and he was immediately escorted from the premises and his access to the premises was terminated. The security system printout disclosed he accessed approximately 10 sites between the hours of 10:31 a.m. and 11:13 a.m. on January 15, 2004, approximately 20 sites between 6:13 p.m. and 7:30 p.m. on January 16, 2001, approximately 30 sites between 7:25 p.m. and 8:27 p.m. on January 18, 2001, and approximately 40 sites between 5:34 p.m. and 7:49 p.m. on January 19, 2001. He also accessed a single site for thirty seconds at 1:36 p.m. on January 16, 2001. The great majority of the sites were only accessed for a few seconds, although some were viewed for nearly 30 minutes. Applicant testified he accessed the sites out of curiosity.

Applicant was required to record the hours he worked on a daily basis on a timecard he was required to obtain from and return to his employer's place of business during each pay period.[(3)] He failed to record his daily hours worked on a number of days between January 15, 2001, and January 26, 2001 because of what he attributes to either laziness or sloppiness.

Applicant's employer conducted an investigation of the infractions after being notified of the alleged offenses and Applicant's termination by the other contractor. Applicant admitted accessing the pornographic web sites and claimed they were accessed after work hours or during his lunch hour. The security detection system printout, as detailed above, for the most part confirms the sites were accessed outside of what would be considered normal work hours or in the proximity of what may have been a lunch hour. However, no definitive evidence, other than Applicant's statement, exists as to whether or not the sites were accessed during working hours because he was allowed to work an irregular schedule.

Applicant claimed he was unaware of any employer policy he violated by accessing the pornographic sites outside work hours on their computer. The employer did not have an internet policy in effect at the time, and thus the investigation concluded he was actually unaware of any company policy that would have prohibited him from using a company computer to access pornographic web sites outside working hours. The investigation also concluded that Applicant had not committed timecard fraud by failing to record his hours worked on a daily basis.

Although Applicant's employer concluded he had not violated an internet use policy or engaged in timecard fraud, it did impose disciplinary action upon him because he had been perceived by one of its costumers as not performing his job in a professional manner. Applicant was placed on leave without pay from January 27, 2001 until February 25, 2001. He was also counseled and issued a final warning that any future violation of his employer's policies would result in immediate dismissal. There has been no subsequent misconduct by Applicant.

POLICIES

The Directive sets forth adjudicative guidelines to consider when evaluating a person's eligibility to hold a security clearance. Chief among them are the Disqualifying Conditions (DC) and Mitigating Conditions (MC) for each applicable guideline. Additionally, each clearance decision must be a fair and impartial commonsense decision based upon the relevant and material facts and circumstances, the whole person concept, and the factors listed in ¶ 6.3.1 through ¶ 6.3.6 of the Directive. Although the presence or absence of a particular condition or factor for or against clearance is not outcome determinative, the adjudicative guidelines should be followed whenever a case can be measured against this policy guidance. Considering the evidence as a whole, Guideline M, pertaining to misuse of information technology systems, Guideline E, pertaining to personal conduct, and Guideline D, pertaining to sexual behavior, with their respective DC and MC, are most relevant in this case.

BURDEN OF PROOF

The sole purpose of a security clearance decision is to decide if it is clearly consistent with the national interest to grant or continue a security clearance for an applicant.(4) The government has the burden of proving controverted facts.(5) The burden of proof in a security clearance case is something less than a preponderance of evidence(6), although the government is required to present substantial evidence to meet its burden of proof.(7) "Substantial evidence is more than a scintilla, but less than a preponderance of the evidence."(8) Once the government has met its burden, the burden shifts to an applicant to present evidence of refutation, extenuation, or mitigation to overcome the case against him.(9) Additionally, an applicant has the ultimate burden of persuasion to obtain a favorable clearance decision.(10)

No one has a right to a security clearance(11) and "the clearly consistent standard indicates that security clearance determinations should err, if they must, on the side of denials."(12) Any reasonable doubt about whether an applicant should be allowed access to classified information must be resolved in favor of protecting national security.(13)

CONCLUSIONS

Under Guideline M, noncompliance with rules, procedures, guidelines or regulations pertaining to information technology systems may raise security concerns about an individual's trustworthiness, willingness, and ability to properly protect classified systems, networks, and information.

Applicant's employer conceded following its investigation and through the hearing testimony of its senior executives that there was no policy in effect in January 2001 that prohibited an employee from using a company-owned computer to visit a pornographic web site outside work hours. There is no evidence to establish Applicant used his computer to do so during his working hours, although the timing of the use on January 15, 2001, and the 30 second use on January 16, 2001 are suspect. Regardless, Applicant's conduct, while exhibiting extremely poor judgment, did not implicate any disqualifying condition under Guideline M.

To the extent Applicant's conduct may have violated the intent of Guideline M, even if it did not violate any specific disqualifying condition, that conduct is substantially outweighed by the facts that it occurred three and one-half years ago, over a very short period of time, in the course of an otherwise excellent career. Applicant is entitled to credit under Mitigating Conditions (MC) 1: *The misuse was not recent or significant* and MC 4: *The misuse was an isolated event*. Applicant has mitigated whatever security concerns may have existed under Guideline M.

Under Guideline E, personal conduct is always a security concern because it asks the central question if a person's past conduct justifies confidence the person can be trusted to properly safeguard classified information.

Applicant's conduct in accessing pornographic web sites on his employer's computer while working in a customer's facility is a clear demonstration of unquestionably poor judgment. Even though his employer did not have a policy that prohibited such use and the use itself was not criminal, Applicant's failure to comprehend and appreciate how that use would be viewed by the customer placed in question whether he is a person who could be trusted. Further, his failure to record the hours he worked, as required by applicable DoD regulations, even though it did not rise to the level of timecard fraud, showed his willingness to disregard rules.

Disqualifying Conditions (DC) 1: *Reliable, unfavorable information provided by associates, employers, coworkers, neighbors, and other acquaintances*; DC 4: *Personal conduct or concealment of information 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* and DC 5: *A pattern of dishonesty or rule violations, including violation of any written or recorded agreement made between the individual and the agency* are all applicable.

Applicant terminated his pornographic web surfing before it was discovered. His misconduct was quickly discovered, and he was just as quickly severely disciplined for his transgressions. Most important, the testimony of his employer's senior management establishes that he learned from his mistakes and they are extremely unlikely to ever be repeated. Further, it once again should be pointed out that his misconduct occurred over a very brief and isolated period of time in what has otherwise been an excellent career. I have considered all Guideline E mitigating conditions and find that MC 5: *The individual has taken positive steps to significantly reduce or eliminate vulnerability to coercion, exploitation, or duress* applies in this case. Considering the total evidence presented in this case, I find Applicant has mitigated the security concerns that existed under Guideline E.

Sexual behavior is a security concern if it involves a criminal offense, may subject the individual to coercion, exploitation, or duress or reflects a lack of judgment or discretion.

Applicant credibly testified he viewed the various pornographic web sites out of curiosity. Although those sites contained graphic sexual images, there is no evidence any of them contained child pornography or other criminal content. There also is no evidence that this was compulsive behavior on the part of Applicant. While arguably DC 3: *Sexual behavior that causes an individual to be vulnerable to coercion, exploitation, or duress* could be said to apply, I do not find this the type of behavior contemplated as included under Guideline D. It is appropriately considered under Guideline E as noted above.

To the extent that Applicant's conduct may be deemed to be of concern under Guideline D, he is entitled to credit for the applicability of MC 2: *The behavior was not recent and there is no evidence of subsequent conduct of a similar nature* and MC 4: *The behavior no longer serves as a basis for coercion, exploitation, or duress*. Applicant has mitigated whatever security concerns may have existed under Guideline D.

FORMAL FINDINGS

SOR ¶ 1-Guideline M: For the Applicant

Subparagraph a: For the Applicant

SOR ¶ 2-Guideline E: For the Applicant

Subparagraph a: For the Applicant

Subparagraph b: For the Applicant

SOR ¶ 1-Guideline D: For the Applicant

Subparagraph a: For the 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 or continue a security clearance for Applicant. Clearance is granted.

Henry Lazzaro

Administrative Judge

1. This action was taken under Executive Order 10865 and DoD Directive 5220.6, dated January 2, 1992, as amended and modified (Directive).

2. Applicant waived the 15 day notice requirement imposed by Enclosure 3 of the Directive. (Tr. pp. 8-10)

3. This requirement is imposed by government regulations upon defense contractors.

4. ISCR Case No. 96-0277 (July 11, 1997) at p. 2.

5. ISCR Case No. 97-0016 (December 31, 1997) at p. 3; Directive, Enclosure 3, Item E3.1.14.

6. *Department of the Navy v. Egan* 484 U.S. 518, 531 (1988).

7. ISCR Case No. 01-20700 (December 19, 2002) at p. 3 (citations omitted).

8. ISCR Case No. 98-0761 (December 27, 1999) at p. 2.

9. ISCR Case No. 94-1075 (August 10, 1995) at pp. 3-4; Directive, Enclosure 3, Item E3.1.15.

10. ISCR Case No. 93-1390 (January 27, 1995) at pp. 7-8; Directive, Enclosure 3, Item E3.1.15

11. *Egan*, 484 U.S. at 528, 531.

12. Id at 531.

13. *Egan*, Executive Order 10865, and the Directive.