KEYWORD: Information Technology; Personal Conduct

DIGEST: Applicant is a 45-year-old test engineer who has worked for a government contractor since 2002. He is retired from the Marine Corps after 20 years of honorable service. Applicant is married with two teenage children. Applicant accessed on his government furnished computer pornographic websites. Applicant was punished by his employer. Applicant had never accessed such sites before his actions or since. Applicant told his wife, children, in-laws and friends of his transgressions. Applicant has admitted his error in judgment. Applicant has successfully mitigating the security concerns regarding Guideline M, misuse of information technology systems, and Guideline E, personal conduct. Clearance is granted.

CASENO: 04-00423.h1

DATE: 11/23/2005

DATE: November 23, 2005

In Re:

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

Applicant for Security Clearance

ISCR Case No. 04-00423

DECISION OF ADMINISTRATIVE JUDGE

CAROL G. RICCIARDELLO

APPEARANCES

FOR GOVERNMENT

Rita C. O'Brien, Esq., Department Counsel

FOR APPLICANT

Pro Se

SYNOPSIS

Applicant is a 45-year-old test engineer who has worked for a government contractor since 2002. He is retired from the Marine Corps after 20 years of honorable service. Applicant is married with two teenage children. Applicant accessed on his government furnished computer pornographic websites. Applicant was punished by his employer. Applicant had never accessed such sites before his actions or since. Applicant told his wife, children, in-laws and friends of his transgressions. Applicant has admitted his error in judgment. Applicant has successfully mitigating the security concerns regarding Guideline M, misuse of information technology systems, and Guideline E, personal conduct. Clearance is granted.

STATEMENT OF CASE

On February 24, 2005, the Defense Office of Hearings and Appeals (DOHA) issued to Applicant a Statement of Reasons (SOR) stating they were unable to find that it is clearly consistent with the national interest to grant or continue a security clearance.[(1)] The SOR, which is in essence the administrative complaint, alleged security concerns under Guideline M, misuse of information technology systems, and Guideline E, personal conduct.

In a sworn statement, dated April 8, 2005, Applicant responded to the SOR allegations, and requested a hearing. In his SOR response, Applicant admitted all the allegations in the SOR.

The case was assigned to me on September 22, 2005. A notice of hearing was issued on September 28, 2005, scheduling the hearing for October 18, 2005. The hearing was conducted as scheduled. The government submitted seven exhibits that were marked as Government Exhibits (GE) 1-7. The exhibits were admitted into the record without objection. Applicant testified on his behalf and submitted nine exhibits that were marked as Applicant's Exhibits (AE) A through I.

The exhibits were admitted into the record without objection. The transcript was received on October 31, 2005.

FINDINGS OF FACT

Applicant's admissions to the allegations in the SOR, are incorporated herein. In addition, after a thorough and careful review of the pleadings, exhibits, and testimony, I make the following findings of fact:

Applicant is a 45-year-old test engineer who has worked for a government contractor in that capacity since 2002. Applicant has been married for 20 years, and has a 17-year-old daughter, and a 15-year-old son. Applicant served in the Marine Corps from 1982 to 2002, retiring honorably as a Major. Applicant has held a security clearance since 1985, without incident.

While working for a government contractor Applicant was furnished a government-issued computer. Applicant worked for the contractor on a military base. Applicant's computer did not have access to classified information or sensitive information. Applicant had difficulty transitioning from the pace of military life to that of civilian life. While at work, in approximately November 2002, Applicant became bored at certain times and began surfing the internet. Although it was not his original intention to access pornographic websites, he stumbled upon some pornographic sites. Applicant accessed pornographic websites from November 2002 until May 2003, when he was confronted by his employer. The frequency in which Applicant would access the websites would depend on his work load. If he was busy he might not access them during a week. If things were slow he might access them several times a day.

Upon being confronted by his employer, Applicant admitted his transgressions. He was reprimanded by his employer and his 2003 bonus was withheld, and his 2004 expected merit increase was reduced by at least one percent. Applicant was retained by the company and warned that any further transgressions would result in employment termination. Despite the punishment Applicant received, he continued to perform his duties in an exemplary manner and it was reflected as such on his performance appraisals.[(2)]

Applicant testified credibly and admitted that he accessed unauthorized websites of a pornographic nature. Applicant has no other adverse actions in his past. Applicant's actions showed a lack of judgment, and were totally out of character. Applicant admitted he made a terrible mistake.

Applicant informed his wife of what he had done. She was shocked and disappointed, but has remained committed to him. Applicant informed his two teenage children that he inappropriately viewed pornographic material at work and that his transgressions could cost him his job. They too were disappointed, but support him. Applicant informed his wife's parents and asked for their forgiveness. They did forgive him and pray for him. Applicant did not tell his parents

because his father suffers from Alzheimer's disease and his mother has the responsibility of caring for him. Applicant felt his father would not understand and he did not want to burden his mother with additional stresses. Some of Applicant's friends are also aware of what he did. Applicant does not hide what he did and readily admits to his actions. Applicant was informed by his supervisor that he should not tell other employees that he works with about what happened. Although admittedly embarrassed Applicant stated "I don't hide and I don't not tell the truth, ..."[(3)]

Applicant credibly testified that he had never accessed anything inappropriate while serving with the Marines, nor has he accessed anything inappropriate since he was caught in May 2003. If Applicant gets bored he uses his time in a more productive way that benefits his employer.

Although Applicant does admit to intentionally clicking on sites that contained pornographic images, he did not intentionally save images to be viewed later or put into files. Rather the computer did save the images as part of its normal function. Applicant was not aware that the computer automatically saved the images he accessed.

Applicant is viewed by his facility security officer as an honest man, who never denied what he did wrong. She does not believe him to be a security risk. Applicant is also viewed by some people he works with as a trustworthy and reliable employee, despite having made a grave error in judgment. It is believed that his actions are inconsistent with his character. The fact that he readily admitted his mistake and has not tried to hide his transgressions is also attributable to his integrity. Applicant has an outstanding reputation with his employer, and after the incident he received an outstanding performance award for his support of a program he was working on.

POLICIES

Enclosure 2 of the Directive sets forth adjudicative guidelines to be considered in evaluating a person's eligibility to hold a security clearance. Included in the guidelines are disqualifying conditions (DC) and mitigating conditions (MC) applicable to each specific guideline. Considering the evidence as a whole, Guideline M, pertaining to misuse of information technology systems, and Guideline E, personal conduct considerations, with their respective DC and MC, apply in this case. Additionally, each security clearance decision must be a fair and impartial commonsense decision based on the relevant and material facts and circumstances, the whole-person concept, along with the factors listed in the Directive. Specifically these are: (1) the nature and seriousness of the conduct and surrounding circumstances; (2) the frequency and recency of the conduct; (3) the age of the applicant; (4) the motivation of the applicant, and the extent to which the conduct was negligent, willful, voluntary, or undertaken with knowledge of the consequences; (5) the absence or presence of rehabilitation; and (6) the probability that the circumstances or conduct will continue or recur in the future. 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.

The sole purpose of a security clearance determination 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 is something less than a preponderance of evidence.(6) 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.(7) Additionally, an applicant has the ultimate burden of persuasion to obtain a favorable clearance decision.(8)

No one has a right to a security clearance(9) and "the clearly consistent standard indicates that security clearance determinations should err, if they must, on the side of denials."(10) Any reasonable doubt about whether an applicant should be allowed access to sensitive information must be resolved in favor of protecting such sensitive information.(11) The decision to deny an individual a security clearance is not necessarily a determination as to the loyalty of an applicant.(12) 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.

Based upon consideration of the evidence, I find the following adjudicative guidelines most pertinent to the evaluation of the facts in this case:

Guideline M-Misuse of information technology systems and noncompliance with rules, procedures, guidelines or regulations pertaining to these systems may raise security concerns about an individual's trustworthiness, willingness, and ability to properly protect classified systems, networks, and information. Information technology systems include all related equipment used for the communication, transmission, processing, manipulation, and storage of classified or sensitive information.

Guideline E-Personal Conduct is a security concern when an individual's conduct involves questionable judgment, untrustworthiness, unreliability, lack of candor, dishonesty, or unwillingness to comply with rules and regulations that could indicate that the person may not properly safeguard classified information.

Conditions that could raise a security concern and may be disqualifying, as well as those which would mitigate security concerns, pertaining to the adjudicative guidelines are set forth and discussed in the conclusions below.

CONCLUSIONS

I have carefully considered all the facts in evidence and the legal standards. The government has established a *prima facie* case for disqualification under Guideline M and Guideline E.

Based on all the evidence, Misuse of Information Technology Systems Disqualifying Condition (MI DC) E2.A13.1.2.3 (*Removal (or use) of hardware, software or media from any information technology system without authorization, when specifically prohibited by rules, procedures, guidelines, or regulations)* is applicable. Applicant accessed pornographic material on his government furnished computer in violation of government regulations.

I have considered all the mitigating conditions under Misuse of Information Technology Systems Mitigating Conditions (MI MC) to include MI MC E2.A13.1.3.1 *(The misuse was not recent or significant);* MI MC E2.A13.1.3.2 (*The conduct was unintentional or inadvertent);* MI MC E2.A13.1.3.3 (*The introduction or removal of media was authorized);* and MI MC E2.A13.1.3.4 *(The misuse was an isolated event).* I conclude MI MC E2.A13.1.3.1 applies. Applicant's actions last occurred in May 2003, over two and a half years ago. Since that time Applicant has advised his wife, children, in-laws and friends of what he did. I have considered the general mitigating guidelines when applying the facts of this case to the regulation. I especially considered the recency of the conduct,[(13)] over two and a half years ago. I have considered the absence or presence of rehabilitation,[(14)] in this case Applicant readily admitted his error in judgment, acknowledged it to his family, vowed never to do it again, and continued to perform in an exemplary manner since being punished. I have also considered the probability that the circumstances or conduct will continue or recur in the future. Applicant's actions since the incident, his work record, his remorse and actions in telling those who are very close to him, along with his credible testimony shows he is totally committed to never being involved in such a situation again. I have considered all of the other mitigating conditions listed above and find they do not apply. However, I do find that Applicant has successfully mitigated the security concerns regarding his conduct as previously discussed.

Considering the evidence, Personal Conduct Disqualifying Condition (PC DC) E2.A5.1.2.1 *Reliable, unfavorable information provided by associates, employers, coworkers, neighbors, and other acquaintances);* PC DC E2.A5.1.2.4 (*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 PC DC E2.A5.1.2.5 (*A pattern of dishonesty or rule violations, including violation of any written or recorded agreement made between the individual and the agency)* apply in this case. Applicant accessed unauthorized pornographic websites on his government computer. His supervisors became aware of his actions and his conduct is of the type that could increase his vulnerability to coercion or exploitation. Applicant did this over a period of time which showed a pattern of rules violation.

I have considered all the mitigating conditions and specifically considered Personal Conduct Mitigating Condition (PE MC) E2.A5.1.3.5 (*The individual has taken positive steps to significantly reduce or eliminate vulnerability to coercion, exploitation, or duress)* and conclude it applies. Although Applicant's actions and violations were not a one time aberration, Applicant has accepted responsibility, continued to work diligently for his employer, and has told those closest to him, his family and friends, of his deeds. These positive steps and Applicant's credible assertions that he has

ceased all such activity, had never done it before these occurrences and has never done it since, significantly reduce his vulnerability to coercion and exploitation. Based on these facts and the analysis previously provided, I conclude Applicant has successfully mitigated the security concerns regarding his personal conduct.

In all adjudications, the protection of our national security is the paramount concern. The objective of the security-clearance process is the fair-minded, commonsense assessment of a person's life to make an affirmative determination that the person is eligible for a security clearance. Indeed, the adjudicative process is a careful weighing of a number of variables in considering the "whole person" concept. It recognizes that we should view a person by the totality of their acts, omissions, motivations and other variables. Each case must be adjudged on its own merits, taking into consideration all relevant circumstances, and applying sound judgment, mature thinking, and careful analysis.

I considered all the evidence provided and also considered the "whole person" concept in evaluating Applicant's risk and vulnerability in protecting our national interests. There is no question that Applicant exercised very poor judgment in his actions that give rise to this case. However, when viewing the whole person, I must also consider Applicant's 20 years of honorable military service, the fact he has held a security clearance since 1985 without incident, his continued commitment to his work despite being embarrassed about his actions, the fact that he has confessed his transgressions to his wife, children, in-laws and friends, are all important factors to consider. I find Applicant has rehabilitated himself and it is highly unlikely that he will be involved in any adverse actions in the future. Applicant has successfully mitigated the security concerns regarding the misuse of information technology systems and personal conduct.

FORMAL FINDINGS

Formal Findings for or against Applicant on the allegations set forth in the SOR, as required by Section E3.1.25 of Enclosure 3 of the Directive, are:

Paragraph 1 Misuse of Information Technology FOR THE APPLICANT

Systems (Guideline M)

Subparagraph 1.a. For the Applicant

Paragraph 2 Personal Conduct (Guideline E) FOR THE APPLICANT

Subparagraph 2.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.

Carol. G. Ricciardello

Administrative Judge

1. This action was taken under Executive Order 10865, dated February 20, 1960, as amended, and DoD Directive 5220.6, dated January 2, 1992, as amended and modified (Directive).

2. Applicant Exhibit (AE) G-I.

3. Transcript (TR.) at 30.

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

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

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

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

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

9. *Egan*, 484 U.S. at 531.

10. *Id*.

11. *Id*.; Directive, Enclosure 2, ¶ E2.2.2.

12. Executive Order 10865 § 7.

13. DoD Regulation 5220.6 at 6.3.2.

14. *Id.* at 6.3.5.