KEYWORD: Information Technology; Personal Conduct

DIGEST: Applicant is a 37-year-old software engineer for a defense contractor. At his previous job, Applicant conducted a test, without authorization, on a co-worker's computer that caused the computer to crash. Applicant failed to advise his supervisor or co-worker that he was conducting the test. He knew at the time that if the test was successful, it would crash the computer. Applicant did not immediately notify either the supervisor or co-worker after the computer crashed. Applicant made prank phone calls to the same co-worker. Applicant mitigated Guideline M, pertaining to misuse of information technology systems, but failed to mitigate Guideline E, pertaining to personal conduct. Clearance is denied.

CASENO: 02-26331.h1

DATE: 04/25/2005

DATE: April 25, 2005

In re:

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

Applicant for Security Clearance

ISCR Case No. 02-26331

DECISION OF ADMINISTRATIVE JUDGE

CAROL G. RICCIARDELLO

APPEARANCES

FOR GOVERNMENT

Rita O'Brien, Esq., Department Counsel

FOR APPLICANT

Tom Blount, Esq.

SYNOPSIS

Applicant is a 37-year-old software engineer for a defense contractor. At his previous job, Applicant conducted a test, without authorization, on a co-worker's computer that caused the computer to crash. Applicant failed to advise his supervisor or co-worker that he was conducting the test. He knew at the time that if the test was successful, it would crash the computer. Applicant did not immediately notify either the supervisor or co-worker after the computer crashed. Applicant made prank phone calls to the same co-worker. Applicant mitigated Guideline M, pertaining to misuse of information technology systems, but failed to mitigate Guideline E, pertaining to personal conduct. Clearance is denied.

STATEMENT OF CASE

On March 8, 2004, 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, alleges security concerns under Guideline E, personal conduct, and Guideline M, misuse of information technology systems.

In a sworn statement, dated March 26, 2004, Applicant responded to the SOR allegations, and requested a hearing. In his SOR response, Applicant admitted some allegations contained in the SOR and denied others. Applicant also provided explanations in an effort to extenuate and mitigate the security concerns raised by the allegations.

The case was originally assigned to another judge on December 1, 2004. Due to case load considerations it was reassigned to me on December 8, 2004. A notice of hearing was issued on March 9, 2005, scheduling the hearing for March 30, 2005. The hearing was conducted as scheduled. The government submitted four exhibits that were marked as Government Exhibits (GE) 1-4, and admitted into the record. The Applicant testified, on his own behalf, and submitted 7 exhibits that were marked as Applicant's Exhibits (AE) A-G, and were admitted into the record. The transcript was received on April 11, 2005.

FINDINGS OF FACT

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

Applicant is 37 years old and graduated from college in 1995. He is a software engineer and has worked in various computer related jobs since graduating from college. Applicant presently works for a defense contractor, and in the past held a secret security clearance when he was employed by a different defense contractor. He does not currently hold a security clearance.

Applicant was employed as a software engineer by Company A from 1997 until March 1999. Company A is a large national company and in the location where Applicant was employed there were approximately two thousand employees. Applicant's work assignment was to test software. Company A was not a defense contractor. Applicant did not work with sensitive or classified material or computers.

In 1999, through Applicant's research of trade material, he learned there might be a potential flaw in the main operating system that was a product of Company A. Applicant decided to conduct a test to see if the flaw existed. Applicant did not advise his supervisor he was conducting the test. Applicant needed two computers to conduct the test, so he used his company-issued computer and a company-issued computer that was assigned to a co-worker. Applicant did not request permission or advise the co-worker that he was using his computer to conduct the test. The co-worker was not present when Applicant conducted the test. Essentially, Applicant's test involved overloading the computer system to determine if the system would "freeze" or "crash." When Applicant's test was successful, he crashed his co-worker's computer. Then Applicant rebooted the co-worker's computer.

Applicant claims he did not believe he needed permission to conduct the test as it was part of his job to conduct tests. Applicant claims tests were performed on the computers on a regular basis. Applicant disputes that any of the co-worker's work was destroyed, but admits he did not know what, if any, work product was on the co-worker's computer; and he did not investigate or ask if any was missing. Applicant did not advise the co-worker of the test he performed on the co-worker's computer until he was confronted with the information by his supervisor. Applicant admits he would want to know if someone had crashed his computer. Applicant admits in his sworn statement of April 25, 2002, and in his sworn answer to the SOR, that "without authorization" he used his co-worker's computer. However, while testifying at his hearing, Applicant denied he conducted the test "without authorization." [(2)]He stated, "I don't believe it was unauthorized."[(3)] "I was not told not to do anything like this."[(4)] Applicant testified he did not know he was unauthorized."[(5)] These statements are in direct conflict with his previous sworn statements. I find Applicant's testimony to be evasive and not credible.

Applicant did not report the "test" results to his supervisor. Rather, the following day, he was directed to report to his supervisor. Applicant stated in his sworn answer to the SOR, "I admit I was discovered by my former employer ... as the person responsible for intentionally causing a coworker's computer to 'crash' in about early 1999 by overloading the . . . operating system." Applicant denies he intended to or did cause destruction of the co-worker's work. Applicant admits that his supervisor was very angry by Applicant's actions.

Also, Applicant was confronted by his supervisor regarding telephone calls he made to the same co-worker whose computer Applicant conducted the test. Applicant's supervisor advised Applicant that the information technology department had traced the crash and phone calls to Applicant. Applicant admitted making prank telephone calls to the same co-worker by calling him up and hanging up. He did this over a two to three month period. Applicant claims these calls were a joke. Applicant did not know whether the co-worker knew if the prank calls were made by Applicant. These phone calls were a form of harassment. Applicant denied he sent threatening emails and/or messages to the same co-worker. Applicant claims that this co-worker was a good friend. Applicant offered his resignation to his supervisor. He was advised to wait a day. The following day, after a meeting of Applicant's supervisors, it was decided that it would be in everyone's best interest for Applicant to voluntarily resign. Applicant resigned immediately.

Applicant's performance evaluations from Company A reflect that Applicant kept management informed and provided weekly status reports.[(6)] He planned his work based on top level guidance provided by his technical lead and when a technology or organizational problem was encountered Applicant consulted the lead to resolve the issue.[(7)]

Applicant received excellent performance evaluations from Company A and his new employer. Applicant provided character references that reflect Applicant is a dedicated worker and none of those presenting letters have witnessed any actions that would indicate Applicant is untrustworthy, irresponsible or reckless. Applicant's character is held in high regard by those submitting letters.

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 E, pertaining personal conduct, and Guideline M, pertaining to misuse of information technology system, 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.(8) The government has the burden of proving controverted facts.(9) The burden of proof is something less than a preponderance of evidence.(10) 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.(11) Additionally, an applicant has the ultimate burden of persuasion to obtain a favorable clearance decision.(12)

No one has a right to a security clearance(13) and "the clearly consistent standard indicates that security clearance determinations should err, if they must, on the side of denials."(14) Any reasonable doubt about whether an applicant should be allowed access to sensitive information must be resolved in favor of protecting such sensitive information.(15) The decision to deny an individual a security clearance is not necessarily a determination as to the loyalty of an applicant.(16) 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 E-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.

Guideline M-Noncompliance with rules, procedures, guidelines or regulations pertaining to information technology systems may raise security concerns about an individual's trustworthiness, willingness, or 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.

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 E, but has failed to establish a *prima facie* case for disqualification under Guideline M.

Based on all the evidence, under Guideline M, the government failed to establish its case, as none of the four disqualifying conditions apply. Applicant's actions while working for Company A involved poor judgment resulting in him leaving Company A, but the evidence does not show his actions involved using an "information technology system" which is a necessary element of each of the four disqualifying conditions. In other words, there is no evidence establishing Applicant's actions were on a computer that was part of a system used for classified or sensitive information. Given this failure of proof, Guideline M is decided for Applicant.

Considering the evidence, Personal Conduct Disqualifying Condition (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)* applies in this case. Applicant conducted a test on a co-worker's computer: when the test was successful, the computer crashed. His personal conduct in this regard would certainly negatively affect his personal, professional and community standing, especially in a computer dependent workplace. The nature of Applicant's phone calls to a co-worker, were harassing because they occurred over a two to three month period, and took place in a work environment. Also, Applicant did not informed the co-worker that he was the one making the calls, thereby potentially creating concern and fear as to who might be making the calls. The government failed to provide a prima facie case that threatening emails were sent by Applicant to a co-worker.

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 does not apply.

Applicant's exhibited a serious error in judgment. The fact Applicant performed this act without advising the co-worker or supervisor before or immediately after is a serious lapse in judgment. Applicant's personnel history, reflected in his performance evaluations, states that Applicant kept management informed and sought out top level guidance with problems when technical or organizational issues were encountered. Applicant deliberately did not seek guidance when conducting what he admitted was an incredibly significant test for Company A. The fact that he would conduct the test on a co-worker's computer, reflects not only very questionable judgment, but also a suspicious and questionable motive regarding his actions as he was also making prank phone calls to the co-worker. Applicant was 31 years old at the time of these actions, well beyond the age of youthful indiscretion. His actions were intentional as he knew that the actual test he conducted, if successful, would crash the computer. These facts (along with Applicant's inconsistent testimony with his sworn statements) reflect an absence of rehabilitation or behavior changes. Applicant has failed to mitigate the

security concerns regarding his personal conduct. Accordingly, Guideline E is decided against Applicant.

I have considered all the evidence in this case and the credibility of the Applicant. I have also considered the "whole person" concept in evaluating Applicant's risk and vulnerability in protecting our national interests. I am persuaded by the totality of the evidence in this case that it is not clearly consistent with the national interest to grant Applicant a security clearance. The government failed to establish a prima facie case regarding misuse of information technology systems. Therefore, Guideline M is decided for Applicant. Applicant failed to mitigate the security concerns caused by personal conduct considerations, and accordingly Guideline E is decided against Applicant.

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. Personal Conduct: (Guideline E) AGAINST THE APPLICANT

Subparagraph 1.a. Against the Applicant

Subparagraph 1.b. Against the Applicant

Paragraph 2. Misuse of Information: FOR THE APPLICANT

Technology Systems (Guideline M)

Subparagraph 2.a. For the 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 or continue a security clearance for Applicant. Clearance is denied.

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. Tr. at 50-52.

3. Tr. at 51.

4. Id. at 52

5. Id.

6. GE 3 at 14.

7. Id.

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

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

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

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

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

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

14. Id.

15. Id.; Directive, Enclosure 2, ¶ E2.2.2.

16. Executive Order 10865 § 7.