DATE: February 16, 2005

In Re:

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

Applicant for Security Clearance

ISCR Case No. 03-09001

DECISION OF ADMINISTRATIVE JUDGE

MATTHEW E. MALONE

APPEARANCES

FOR GOVERNMENT

Juan Rivera, Esquire, Department Counsel

FOR APPLICANT

Pro Se

SYNOPSIS

During a two-week period in 1997, Applicant improperly used his company's computer system resulting in the compromise of passwords and other security mechanisms. He resigned his position and was eventually charged with and pled guilty in federal court to a single count of felony computer fraud. During the next 12 months, he was terminated from two subsequent jobs when those employers learned of the charges. However, he has since mitigated the security concerns under Guideline E (personal conduct), Guideline J (criminal conduct), and Guideline M (misuse of information technology systems). Accordingly, his request for clearance is granted.

STATEMENT OF THE CASE

On January 26, 2004, the Defense Office of Hearings and Appeals (DOHA) issued a Statement of Reasons (SOR) to Applicant. The SOR informed Applicant that DOHA adjudicators could not make a preliminary affirmative finding that it is clearly consistent with the national interest to continue Applicant's security clearance.[(1)] The SOR alleges facts that raise security concerns under Guideline E (Personal Conduct), Guideline J (Criminal Conduct), and Guideline M (Misuse of Information Technology Systems).

On February 11, 2004, Applicant responded to the SOR (Answer), wherein he admitted with explanation all of the SOR allegations, and requested a hearing. The case was assigned to me on August 30, 2004. On October 6, 2004, I convened a hearing at which the government submitted seven exhibits (Ex. 1 - 7).[(2)] Applicant submitted six exhibits (Ex. A - F) and the testimony of four witnesses including himself. DOHA received the transcript (Tr.) on October 19, 2004.

FINDINGS OF FACT

I have incorporated Applicant's admissions in his Answer into this decision. After a thorough review of the pleadings, transcript, and exhibits, I make the following additional findings of fact:

Applicant is 33 years old and seeks his first security clearance as part of his employment with a defense contractor.

Since 1998, he has worked as a senior engineer in information technology (IT) systems, a field in which he has a bachelor's and a master's degree. He is currently studying for a doctorate in computer forensics.

Applicant worked in the IT field while he was in school full-time until age 24. He then went to work for a series of companies, sometimes consulting for one firm while holding a full-time position with another. In June1997, Applicant went to work for a large corporation with contracts in the space program. The first manager to whom he was assigned was often busy or out of town. Applicant was generally assigned IT duties related to a particular mission management system, but was often left without direction or with assigned duties that under utilized his skills.

In his previous jobs, Applicant had been involved with IT system security, which, in the early- and mid-1990s was not as defined a facet of IT as it is today. For example, the design and use of system firewalls, a fundamental aspect of most computer networks today, was found primarily in large corporations and government agencies. In early July, 1997, Applicant's manager allowed him to test and examine the mission management system security configuration to identify potential vulnerabilities; however, the manager's guidance was not specific as to how to go about this or how far he could go in testing the system.

Applicant initially audited the mission management system internally by installing a program called "crack" designed to identify easily-breakable passwords, and another program called "snoop" designed to identify external system vulnerabilities. It is not unusual for systems administrators to routinely monitor their systems' weaknesses in this way. Applicant reported his findings on two occasions to one of his superiors.

At some point, Applicant thought it would be helpful to test the mission management system's vulnerability to external unauthorized intrusion. To do this, he hacked his way into the systems of five companies for whom he had either worked before or, in one instance, for whom he was doing outside consulting in addition to his full-time job. He downloaded and used passwords from all but one of those systems to access them from his workstation. He would then, in turn, try to remotely penetrate the mission management system. Applicant did not damage any of the five systems, but his actions resulted in each company having to expend resources to shore up their systems' security.

Applicant's efforts eventually required more processing capacity than his desktop computer could provide, so he employed the high-capacity government computers his company was charged with running and maintaining. On July 27, 1997, the crack program was discovered on the mission management system during routine maintenance and the source was traced back to Applicant's workstation. It was also determined that either the mission management system was logged into at least one of the other five companies or one of the five were logged into the mission management system. These facts were reported to computer security personnel and Applicant's computer was seized.

A subsequent investigation by a government inspector general showed that while Applicant may have had permission to examine internally the system's vulnerabilities, he greatly exceeded his authority by accessing other companies' systems and by using the government's computers to do so. Applicant resigned his position in August 1997.

The government's report was referred to the local U.S. Attorney's office who prosecuted Applicant for unauthorized access of a protected computer system, a felony.[(3)] Applicant eventually pled guilty to one count of computer fraud and was sentenced to serve 180 days home detention, fined, placed on supervised probation for three years, fined, and ordered to pay restitution of about $12,000, an amount roughly equivalent to the time and labor needed to upgrade the security posture of the systems into which he had intruded.

At Applicant's sentencing hearing in July 1998, the Court reduced the amount of restitution by Applicant to the extent he had arranged with two of the companies victimized by his actions to help them restore and improve their systems. Over government objections, the Court also departed from federal sentencing guidelines requiring six months' incarceration in these circumstances and declined the prosecution's request that Applicant be placed in home detention for 180 days. The Court also opined that Applicant exhibited no malicious intent through his actions, but was simply a bright, immature young man who made an ill-advised decision because he had too much time on his hands at work.

After leaving his position in the wake of the inspector general's report, Applicant found work with a national express shipping company and a temporary staffing agency specializing in IT skills. In each case, when Applicant advised his

employer of his prosecution for computer fraud, he was terminated.

In August 1998, Applicant found work that led to his current position, which he has held since December 1998. His co-workers, supervisors, and the company's facility security officer are aware of Applicant's past conduct and his felony conviction. Nevertheless, they recommend him for a position of trust and hold him the highest regard for his honesty, reliability and overall good character. Further, during the Defense Security Service (DSS) background investigation of Applicant, several of the people with whom he had worked at two of the companies whose systems he had illegally accessed vouched for his good work, reliability and character despite their knowledge of what he had done. One former manager offered that Applicant was very accomplished but, having been in school full-time until about age 24, may have been somewhat naive in the workplace.

Applicant has been married for nearly nine years and they have three young children. He is active in his church, and holds a position of trust involving the safeguarding of church funds. He is also charged in this position with protection of sensitive information about fellow church members. He has a spotless record in that regard.

POLICIES

The Directive sets forth adjudicative guidelines[(4)] to be considered in evaluating an Applicant's suitability for access to classified information. The Administrative Judge must take into account both disqualifying and mitigating conditions under each adjudicative issue applicable to the facts and circumstances of each case. Each decision must also reflect a fair and impartial common sense consideration of the factors listed in Section 6.3 of the Directive. The presence or absence of a disqualifying or mitigating condition is not determinative of a conclusion for or against an Applicant. However, specific applicable guidelines should be followed whenever a case can be measured against them as they represent policy guidance governing the grant or denial of access to classified information. Having considered the record evidence as a whole, I conclude the relevant adjudicative guidelines to be applied here are Guideline E (personal conduct), Guideline J (criminal conduct), and Guideline M (misuse of information technology systems).

BURDEN OF PROOF

A security clearance decision is intended to resolve whether it is clearly consistent with the national interest[(5)] for an Applicant to either receive or continue to have access to classified information. The government bears the initial burden of proving, by something less than a preponderance of the evidence, controverted facts alleged in the SOR. If the government meets its burden it establishes a *prima facie* case that it is not clearly consistent with the national interest for the Applicant to have access to classified information. The burden then shifts to the Applicant to refute, extenuate or mitigate the government's case. Because no one has a "right" to a security clearance, the Applicant bears a heavy burden of persuasion.[(6)] A person who has access to classified information enters into a fiduciary relationship with the government based on trust and confidence. The government, therefore, has a compelling interest in ensuring each Applicant possesses the requisite judgement, reliability, and trustworthiness of one who will protect the national interests as his or her own. The "clearly consistent with the national interest" standard compels resolution of any reasonable doubt about an Applicant's suitability for access in favor of the government.[(7)]

CONCLUSIONS

Guideline E (Personal Conduct). Under this guideline, conduct involving questionable judgment, untrustworthiness, unreliability, dishonesty, or unwillingness to comply with rules and regulations may indicate that the person may not properly safeguard classified information.[(8)] Here the government's allegations in SOR paragraph 2, if proved, would significantly undermine the government's confidence in Applicant's judgment, a fundamental facet of the personnel security program.

The government established that Applicant accessed the computer systems at his place of work, as well as at five companies or organizations where Applicant had previously worked, and that he did so without authorization and for improper purposes. (SOR ¶¶2.a and 2.b) The government also established that Applicant had to resign from one job and was fired from two others as a result of his misconduct and subsequent criminal charges. (SOR ¶¶2.c, 2.d, and 2.e) There is some support for his claim he had permission to test security on the system where he worked; however, it is

also clear he exceeded any reasonable interpretation of that authority when he hacked into the IT systems of his former employers and when he used government super computers to carry out his actions. These facts raise the overall concern under this guideline as stated above; they also require application of Guideline E disqualifying condition (DC) 4[(9)] owing to the adverse effect his conduct had on his employment until late 1998.

By contrast, I conclude Applicant has presented sufficient mitigating information to overcome the government's case under Guideline E. His conduct was isolated in that it was a single ongoing event that spanned a brief period in July 1997. It has also been over seven years since that event without any further indication Applicant might repeat his conduct despite clearly having the requisite knowledge and skills to do so. Additionally, Applicant has over several years demonstrated an acceptable degree of reliability and judgment through his church-related duties, which demand a level of discretion and trustworthiness analogous to that required of a clearance holder. Most persuasive, however, is the fact his past employers whose systems were targeted by his actions, as well as his current employer, recommend him for a position of trust. They acknowledge his actions were inappropriate but, based on their knowledge and experience with him, have no doubt he understands his mistakes, feel he has matured a great deal since 1997, and will not again err in this way. Based on application of Guideline E mitigating condition 5,[(10)] and in consideration of the adjudicative factors set forth in Directive, Section E2.2.1,[(11)] I conclude Guideline E for the Applicant.

Guideline J (Criminal Conduct). The security concern under Guideline J is that a person who is willing to disregard the law and risk fines or incarceration may also be willing to disregard rules and regulations governing the protection of classified information.[(12)] In some cases, the criminal activity may consist of a single serious crime. The government has established that Applicant was convicted of a single count of felony computer fraud. (SOR ¶1.a) Guideline J DC 2 [(13)] applies. While the sentencing Court's comments regarding Applicant's lack of bad intent in his actions does not lessen the seriousness of his conduct, the fact the Judge departed as he did from the sentencing guidelines must be taken into account in assessing the security significance of Applicant's conduct. He should have known what he was doing was, at the very least, illegal. He admits knowing at the time he did not have permission to access the systems of his former employers, and, in hindsight, that it was probably illegal to do so. However, it was also clear at the time Applicant made a single, serious mistake out of inexperience and immaturity.

In further mitigation, Applicant's conduct was isolated, was not recent, and there is clear evidence of rehabilitation. Guideline J MC 1,[(14)] MC 2,[(15)] and MC 6[(16)] apply. For these reasons, and in consideration of the same general adjudicative factors discussed under Guideline E, above, I conclude Guideline J for the Applicant.

Guideline M (Misuse of Information Technology Systems). 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. Information technology systems include all related equipment used for the communication, transmission, processing, manipulation, and storage of classified or sensitive information.[(17)] The government established that Applicant violated rules and procedures governing access to a system used to process sensitive information through his employer's system and the systems of former employers. (SOR ¶3.a) The government further established his conduct was illegal and that it included introduction of unauthorized software and manipulation of access resident in those systems. Guideline M DC 1,[(18)] DC 2,[(19)] and DC 4[(20)] apply.

In mitigation, his conduct was not recent and it was isolated. MC 1[(21)] and MC 4[(22)] apply. I have also considered MC 5[(23)] to the extent Applicant made an effort to repair what damage he inflicted on the systems involved; however, his actions may have been well intended but they were not prompt. On balance, however, I conclude Guideline M for the Applicant.

I have carefully weighed all of the evidence in this case, and I have applied the aforementioned disqualifying and mitigating conditions as listed under each applicable adjudicative guideline. I have also considered the whole person concept as contemplated by the Directive in Section 6.3, and as called for by a fair and commonsense assessment of the record before me as required by Directive Section E2.2.3. The record evidence as a whole supports a conclusion that Applicant is not likely to repeat his lapse in judgment of seven years ago and may be relied on to adhere to rules and

regulations intended to help safeguard classified information. Applicant has presented sufficient evidence about his good character and trustworthiness in and out of the workplace to overcome the doubts raised by the government's case.

FORMAL FINDINGS

Formal findings regarding each SOR allegation as required by Directive Section E3.1.25 are as follows:

Paragraph 1, Criminal Conduct (Guideline J): FOR THE APPLICANT

Subparagraph 1.a: For the Applicant

Paragraph 2, Personal Conduct (Guideline E): FOR THE APPLICANT

Subparagraph 2.a: For the Applicant

Subparagraph 2.b: For the Applicant

Subparagraph 2.c: For the Applicant

Subparagraph 2.d: For the Applicant

Subparagraph 2.e: For the Applicant

Paragraph 3, Misuse of IT Systems (Guideline M): For the Applicant

Subparagraph 3.a For the Applicant

DECISION

In light of all the circumstances presented in this case, it is clearly consistent with the national interest to grant or continue a security clearance for the Applicant. Clearance is granted.

Matthew E. Malone

Administrative Judge

1. Required by Executive Order 10865, as amended, and by DoD Directive 5220.6 (Directive), as amended.

2. Exhibit 7 is an index which identifies the other six. As such, it is not a substantive exhibit that affects the outcome of this case.

3. Title 18 U.S.C. § 1030. Fraud and related activity in connection with computers.

4. Directive, Enclosure 2.

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

6. *See Egan,* 484 U.S. at 528, 531.

7. *See Egan;* Directive E2.2.2.

8. Directive, E2.A5.1.1.

9. Directive, 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;

10. Directive, E2.A5.1.3.5. The individual has taken positive steps to significantly reduce or eliminate vulnerability to coercion, exploitation, or duress;

11. E2.2.1. The adjudicative process is an examination of a sufficient period of a person's life to make an affirmative determination that the person is eligible for a security clearance. Eligibility for access to classified information is predicated upon the individual meeting these personnel security guidelines. The adjudicative process is the careful weighing of a number of variables known as the whole person concept. Available, reliable information about the person, past and present, favorable and unfavorable, should be considered in reaching a determination. In evaluating the relevance of an individual's conduct, the adjudicator should consider the following factors:
E2.2.1.1. The nature, extent, and seriousness of the conduct;
E2.2.1.2. The circumstances surrounding the conduct, to include knowledgeable participation;
E2.2.1.3. The frequency and recency of the conduct;
E2.2.1.4. The individual's age and maturity at the time of the conduct;
E2.2.1.5. The voluntariness of participation;
E2.2.1.6. The presence or absence of rehabilitation and other pertinent behavioral changes;
E2.2.1.7. The motivation for the conduct;
E2.2.1.8. The potential for pressure, coercion, exploitation, or duress; and
E2.2.1.9. The likelihood of continuation or recurrence;

12. Directive, E2.A10.1.1.

13. Directive, E2.A10.1.2.2. A single serious crime or multiple lesser offenses.

14. Directive, E2.A10.1.3.1. The criminal behavior was not recent;

15. Directive, E2.A10.1.3.2. The crime was an isolated incident;

16. Directive, E2.A10.1.3.6. There is clear evidence of successful rehabilitation.

17. Directive, E2.A13.1.1.

18. Directive, E2.A13.1.2.1. Illegal or unauthorized entry into any information technology system;

19. Directive, E2.A13.1.2.2. Illegal or unauthorized modification, destruction, manipulation, or denial of access to information residing on an information technology system;

20. Directive, E2.A13.1.2.4. Introduction of hardware, software or media into any information technology system without authorization, when specifically prohibited by rules, procedures, guidelines or regulations;

21. Directive, E2.A13.1.3.1. The misuse was not recent or significant;

22. Directive, E2.A13.1.3.4. The misuse was an isolated event;

23. Directive, E2.A13.1.3.5. The misuse was followed by a prompt good faith effort to correct the situation.