KEYWORD: Security Violations; Information Technology; Sexual Behavior; Personal Conduct; Foreign Influence

DIGEST: Applicant is 44 years old and has worked as a computer specialist for a federal contractor since 1987. From 1998 to 2004, he used his company's internet to access various foreign website to meet women with whom he later engaged in extramarital relationships. In 2003, he was disciplined for failing to secure two hard drives after removing them from an employee's computer. He failed to mitigate the security concerns raised by his security violations, misuse of information technology systems, sexual behavior, personal conduct, and foreign influence. Clearance is denied.

CASENO: 04-06327.h1

DATE: 03/20/2006

DATE: March 20, 2006

In re:

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

Applicant for Security Clearance

ISCR Case No. 04-06327

DECISION OF ADMINISTRATIVE JUDGE

SHARI DAM

APPEARANCES

FOR GOVERNMENT

Jason Perry, Department Counsel

FOR APPLICANT

Pro Se

SYNOPSIS

Applicant is 44 years old and has worked as a computer specialist for a federal contractor

since 1987. From 1998 to 2004, he used his company's internet to access various foreign websites to meet women with whom he later engaged in extramarital relationships. In 2003, he was disciplined for failing to secure two hard drives after removing them from an employee's computer. He failed to mitigate the security concerns raised by his security violations, misuse of information technology systems, sexual behavior, personal conduct, and foreign influence. Clearance is denied.

STATEMENT OF THE CASE

On April 7, 2005, the Defense Office of Hearings and Appeals (DOHA) issued a Statement of Reasons (SOR) to Applicant, under Executive Order 10865, *Safeguarding Classified Information Within Industry*, as amended and modified, and Department of Defense Directive 5220.6, *Defense Industrial Security Clearance Review Program* (Directive), dated January 2, 1992, as amended and modified. The SOR detailed reasons under Guidelines K (Security Violations), (Misuse of Information Technology Systems), B (Foreign Influence), D (Sexual Behavior), and E (Personal Conduct) why DOHA could not make a preliminary affirmative finding under the Directive that it is clearly consistent with the national interest to grant a security clearance to Applicant. DOHA recommended the case be referred to an administrative judge to determine whether a clearance should be granted.

On May 4, 2005, Applicant filed his Answer and elected to have the case decided on the written record in lieu of a hearing. Applicant admitted the allegations in the SOR. On September 27, 2005, Department Counsel prepared a File of Relevant Material (FORM), and provided Applicant with a complete copy on October 28, 2005. Applicant had 30 days from receipt of the FORM to file objections and submit material in refutation, extenuation, or mitigation. Applicant

received the FORM on November 18, 2005, and submitted additional information on November 28, 2005. The case was assigned to me on November 28, 2005.

FINDINGS OF FACT

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

Applicant is 44 years old. Since 1987, he has worked as a computer network support specialist for a federal contractor. (1) In June 1988, he received a secret clearance, which he presently holds. (2) In August 1997, he completed another security clearance application (SCA).

In 1988, Applicant married a Japanese woman, who has retained her Japanese citizenship. They reside in the United States and have two children. (3)

Applicant admitted that from 1998 to March 2004, while at work, he used the company's computer without authorization to access Asian internet website to meet women, in violation of the company's rules and procedures, as alleged in SOR ¶ 2.a.

Applicant admitted that in 1998 he downloaded and installed a software program on his work computer without authorization from his supervisor, as alleged in SOR ¶ 2.b. The program used Japanese characters and he wanted to determine if it could benefit the company. The program expired after 30 days. He did not use it to meet women. (4)

From 1998 until March 2004, Applicant admitted he telephoned and emailed some of the women he became acquainted with through the Asian website, as alleged in SOR ¶ 4.a. He also engaged in extramarital relationships with a Chinese foreign national in 1999 (SOR ¶ 4.b.), a Taiwanese foreign national during 2002 (SOR ¶ 4.c.), another woman in November 2003 (SOR ¶ 4.c.), and a Taiwanese foreign national from March 2003 until March 2004 (SOR ¶ 4.e.). (5)

Applicant admitted that in September 2003, he did not properly secure two secret computer hard drives after he removed

them from an employee's computer. Instead of placing them in a classified safe, he left them outside of the employee's office. He subsequently attempted to locate the classified boot drives at a scrap dealer, but was unable to do so.[(6)] In November 2003, he received a final Written Warning, suspending him for three days without pay for his negligence and requiring him to attend a security briefing session (SOR ¶ 1.a.).[(7)]

In March 2004, Applicant attributed his extramarital activity to a breakdown in his relationship with his wife and his feelings of loneliness and rejection.[(8)] In his ay 2005 Answer, Applicant expressed regret and pain about his misconduct.[(9)] He and his wife subsequently participated in marital counseling where he disclosed his affairs. He is committed to his wife, their marriage, and leading an honest life. He closed his online internet accounts in spring of 2004.[(10)]

POLICIES

Enclosure 2 of the Directive, *Adjudicative Guidelines for Determining Eligibility for Access to Classified Information,* sets forth criteria, which must be evaluated when determining security clearance eligibility. Within those adjudicative guidelines are factors to consider in denying or revoking an individual's request for access to classified information (Disqualifying Conditions), and factors to consider in granting an individual's request for access to classified information (Mitigating Conditions). By recognizing that individual circumstances of each case are different, the guidelines provide substantive standards to assist an administrative judge in weighing the evidence in order to reach a fair, impartial and common sense decision.

The adjudicative process requires thorough consideration and review of all available, reliable information about the applicant, past and present, favorable and unfavorable, to arrive at a balanced decision. Section E2.2. of Enclosure 2 of the Directive describes the essence of scrutinizing all appropriate variables in a case as the "whole person concept." In evaluating the disqualifying and mitigating conduct an administrative judge should consider: (1) the nature, extent, and seriousness of the conduct; (2) the circumstances surrounding the conduct; (3) the frequency and recency of the conduct; (4) the individual's age and maturity at the time of the conduct; (5) the voluntariness of participation; (6) the presence or absence of rehabilitation and other 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.

Granting an applicant's clearance for access to classified information is based on a high degree of trust and confidence in the individual. Accordingly, decisions under the Directive must include consideration of not only the *actual* risk of disclosure of classified information, but also consideration of any *possible* risk an applicant may deliberately or inadvertently compromise classified information. Any doubt about whether an applicant should be allowed access to classified information must be resolved in favor of protecting classified information. Directive ¶ E2.2.2. The decision to deny an individual a security clearance is not necessarily a judgment about an applicant's loyalty. Exec. Or. 10865, § 7. Instead, it is a determination that an applicant has not met the strict guidelines established by the Department of Defense for issuing a clearance.

Initially, the Government must establish, by substantial evidence, conditions in the personal or professional history of the applicant that disqualify, or may disqualify, the applicant from being eligible for access to classified information. *Departments of the Navy V. Egan,* 484 U.S. 518, 531 (1988). The Directive presumes a rational connection between past proven conduct under any disqualifying conditions and an applicant's present security suitability. ISCR Case No. 95-0611 at 2 (App. Bd. May 2, 1996).

Once the Government establishes a disqualifying condition by substantial evidence, the corresponding burden of rebuttal shifts to the applicant to present evidence in refutation, extenuation, or mitigation sufficient to overcome the position of the government. ISCR Case No. 01-20700 at 3 (App. Bd. Dec. 19, 2002); 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 clearance." *Id.*

Based upon the allegations contained in the SOR and a consideration of the evidence as a whole, the following five adjudicative guidelines are pertinent to an evaluation of the facts of this case:

Guideline K - Security Violations: A security concern may exist when a noncompliance with security regulations raises doubt about an individual's trustworthiness, willingness, and ability to safeguard classified information.

Guideline M - Misuse of Information Technology Systems: A security concern may exist when the noncompliance with rules, procedures, guidelines or regulations pertaining to information technology systems raises 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 B - Foreign Influence: A security risk may exist when an individual's immediate family, including cohabitants, and other persons to whom he or she may be bound by affection, influence, or obligations *are not* citizens of the United States *or may* be subject to duress. These situations could create the potential for foreign influence that could result in the compromise of classified information. Contacts with citizens of other countries or financial interests in other countries are also relevant to security determinations if they make an individual potentially vulnerable to coercion, exploitation, or pressure.

Guideline D - Sexual Behavior: Sexual behavior is a security concern if it involves a criminal offense, indicates a personality or emotional disorder, *may subject* the individual *to coercion, exploitation, or duress,* or reflects lack of judgment or discretion.

Guideline E - Personal Conduct: A security concern may exist when 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.

The disqualifying and mitigating conditions, raising either security concerns or mitigating security concerns applicable to this case, are set forth and discussed in the Conclusions section below.

CONCLUSIONS

I have considered all of the facts in evidence and legal standards, including the "whole person" concept, and conclude the following with respect to the allegations set forth in the SOR:

Guideline K: Security Violations

The Government established its case under this guideline. Based on the evidence, Security Violations Disqualifying Condition (SV DC) E2.A11.1.2.2 (*Violations that are deliberate or multiple or due to negligence)* applies to this case. Applicant admitted that in September 2003, he failed to properly secure two company hard drives and was later disciplined for his negligent behavior, as alleged in SOR ¶ 1.a. However, I reviewed all of the mitigating conditions under this guideline, in particular, Security Violation Mitigating Condition (SV MC) E2.A11.1.3.2 (*The actions were isolated or infrequent),* and conclude it is applicable. Because Applicant has worked for his employer for more than 18 years and this is the only violation noted in the record, he has successfully mitigated the security concerns raised by the 2003 security violation. Accordingly, Guideline K is decided for Applicant.

Guideline M: Misuse of Information Technology Systems

The Government established its case under this guideline. Based on the evidence, Misuse of Information Technology Systems Disqualifying Condition (MIS DC) 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) applies. Applicant introduced unauthorized software into the computer system. Although not specifically listed as a disqualifying condition, Applicant failed to comply with his company's rules and regulations, and raised a security concern, by accessing Asian website, as alleged in SOR ¶ 2.a. and ¶ 2.b.

I also considered all of the Misuse of Information Technology Systems Mitigating Conditions (MIS MC), in particular, MIS CM E2.A13.1.3.1 *(The misuse was not recent or significant),* MIS MC E2.A13.1.3.2 (*The conduct was unintentional or inadvertent),* and MIS MC E2.A13.1.3.4 *(The misuse was an isolated event),* and conclude they do not apply. Applicant began consistently misusing the internet at work in 1998 and did not stop until spring of 2004, less than two years ago. As his conduct was recent, intentional and repeated, it is not mitigated under E2.A13.1.3.1, E2.A13.1.3.2, or E2.A13.1.3.4. There is no evidence that he attempted to notify the company of his conduct and correct the situation after he accessed the website, as required under MIS MC E2.A13.1.3.5 (*The misuse was followed by a prompt, good faith effort to correct the situation).* Thus, he did not mitigate the security concerns based on his Misuse of Information Technology Systems, as alleged in SOR ¶ 2.a. and ¶ 2.b. Accordingly, Guideline M is decided against Applicant.

Guideline B: Foreign Influence

The Government established its case under this guideline. Based on the evidence, Foreign Influence Disqualifying Condition (FI DC) E2.A2. 1.2.1 (*An immediate family member, or a person to whom the individual has close ties of affection or obligation, is a citizen of, or resident or present in, a foreign country)* and FI DC E2.A2.1.2.6 *(Conduct which may make the individual vulnerable to coercion, exploitation, or pressure by a foreign government)* apply. Applicant admitted that he met foreign nationals over an Asian internet and engaged in extramarital affairs with some of them. He was involved with a Taiwanese woman for at least a year, indicating he developed an affection for her. These numerous sexual contacts create a potential vulnerability for exploitation of classified information.

I reviewed all of the mitigating conditions under this Guideline, in particular, Foreign Influence Mitigating Condition FI MC E2.A2.1.3.1 (*A determination that the immediate family member(s), (spouse, father, mother, sons, daughter, brothers, sisters), cohabitant, or associate(s) in question are not agents of a foreign power or in a position to be exploited by a foreign power in a way that could force the individual to choose between loyalty to the person(s) involved and the United States)* and conclude it does not apply. Applicant provided little information about the women he met over the internet, including the one he saw for a year. There is no evidence in the record regarding the nature or extent of their contacts or connections to Taiwan or other countries.. Thus, he did not mitigate the security concerns raised by his intimate relations with foreign nationals, who could raise concerns about foreign influence and the compromise of classified information, as alleged in SOR ¶ 3.a. Accordingly, Guideline B is decided against Applicant.

Guideline D: Sexual Behavior

The Government established its case under this guideline. Based on the evidence, Sexual Behavior Disqualifying Condition (SB DC) E2.A4.1.2.3 (*Sexual behavior that causes an individual to be vulnerable to coercion, exploitation, or duress)*, and SB DC E2.A4.1.2.4 (*Sexual behavior of a public nature and/or that which reflects lack of discretion or judgment)* applies. Applicant admitted that for six years he had personal and telephone contact with several foreign women he met through the internet and engaged in extramarital affairs with at least four of them. His wife became aware of his infidelity after he terminated the relationships. There is no evidence that he disclosed his conduct to his employer, friends or other family members. Without that proof his conduct could create a potential vulnerability to coercion or duress. The behavior undeniably demonstrates his lack of good judgment.

I considered all of the Sexual Behavior Mitigating Conditions (SB MC), in particular SB MC E2.A4.1.3.3 (*There is no other evidence of questionable judgment, irresponsibility, or emotional instability),* and conclude none of them apply. In addition to the above conduct, the record documents Applicant's deliberate misuse of his employer's computer system and a negligent breach of security, exemplifying further incidents of poor judgment and irresponsibility. None of the other mitigating conditions are applicable. Thus, Applicant failed to mitigate the security concerns raised by his sexual behavior, as alleged in SOR ¶¶ 4.a. through 4.e. Accordingly, Guideline D is decided against Applicant.

Guideline E: Personal Conduct

The Government established its case under this guideline. Based on 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),* 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 to the facts in this case. Applicant's unauthorized use of the company's internet and risky sexual behaviors are the types of conduct that could impact on his reputation in the community and subject him to duress or blackmail, as contemplated under E2.A5.1.2.4. Additionally, his unauthorized use of the internet at work for six years and his careless breach of security regulations demonstrate a pattern of conduct involving rule violations, which falls under E2.A5.1.2.5.

I considered all of the Personal Conduct Mitigating Conditions, specifically, PC MC E2.A5.1.3.5 (*The individual has taken positive steps to significantly reduce or eliminate vulnerability to coercion, exploitations, or duress)* and conclude it does not apply. While Applicant's remorsefulness and participation in marital counseling are positive steps, I am not persuaded that they are sufficient to mitigate the above disqualification. Although he claims he has divulged his past conduct to his wife, it is unknown if he disclosed it to his employer and friends. Given the recency and the length of time he engaged in the risky and impulsive behaviors, the misconduct is the type that makes him vulnerable to coercion or exploitation. Without objective evidence from a credentialed professional to corroborate his claims of remorse and recognition of wrongdoing, and proof of complete disclosure to other people and his employer, his contriteness does not convince me that he has reduced or eliminated his vulnerability to coercion, exploitation, or duress. Hence, he has failed to mitigate the security concerns raised by his personal conduct, as alleged in SOR ¶ 5.a. and ¶.5.b. Accordingly, Guideline E is decided against Applicant.

I further considered the totality of the evidence in this case, including Applicant's age, work history, the length of time he engaged in the voluntary and risky misconduct, the number of women with whom he became involved, the potential for harm to himself or others, as well as his expression of regret. After doing so, I am persuaded that it is not consistent with the national interest to grant or renew Applicant's security clearance.

For the reasons stated, I conclude Applicant is not eligible for access to classified information.

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: Guideline K (Security Violations) FOR THE APPLICANT

Subparagraph 1.a: For the Applicant

Paragraph 2: Guideline M (Misuse of Information Technology) AGAINST THE APPLICANT

Subparagraph 2.a: Against the Applicant

Subparagraph 2.b: Against the Applicant

Paragraph 3: Guideline B (Foreign Influence) AGAINST THE APPLICANT

Subparagraph 3.a: Against the Applicant

Paragraph 4: (Sexual Behavior) AGAINST THE APPLICANT

Subparagraph 4.a: Against the Applicant

Subparagraph 4.b: Against the Applicant

Subparagraph 4.c: Against the Applicant

Subparagraph 4.d: Against the Applicant

Subparagraph 4.e: Against the Applicant

Paragraph 5: (Personal Conduct) AGAINST THE APPLICANT

Subparagraph 5.a: Against the Applicant

Subparagraph 5.b: Against the Applicant

DECISION

In light of all the circumstances and evidence presented in this case, it is not clearly consistent with the national interest to grant a security clearance to Applicant. Clearance is denied.

Shari Dam

Administrative Judge

1. Item 5 at 1.

2. Item 4 at 8.

3. *Id.* at 4.

4. Item 3 at 4.

5. Item 5 at 9.

6. Item 5 at 11.

7. Item 7.

8. Item 5 at 6.

9. Item 3 at 5.

10. Applicant letter, dated November 18, 2005.