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

DIGEST: Applicant is employed by a defense contractor in a position requiring a security clearance. His duties include monitoring and installing electronic security equipment in U.S. embassies. He failed to mitigate security concerns related to personal conduct, noncompliance with security regulations, sexual behavior, and noncompliance with rules, procedures, and guidelines or regulations pertaining to information systems. Clearance is denied.

CASENO: 03-25340.h1

DATE: 01/26/2006

DATE: January 26, 2006

In Re:

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

Applicant for Security Clearance

ISCR Case No. 03-25340

DECISION OF ADMINISTRATIVE JUDGE

JOAN CATON ANTHONY

APPEARANCES

FOR GOVERNMENT

Stephanie C. Hess, Esq., Department Counsel

FOR APPLICANT

Pro Se

SYNOPSIS

Applicant is employed by a defense contractor in a position requiring a security clearance. His duties include monitoring and installing electronic security equipment in U.S. embassies. He failed to mitigate security concerns related to personal conduct, noncompliance with security regulations, sexual behavior, and noncompliance with rules, procedures, and guidelines or regulations pertaining to information systems. Clearance is denied.

STATEMENT OF THE CASE

The Defense Office of Hearings and Appeals (DOHA) declined to grant or continue a security clearance for Applicant. On May 16, 2005, under the applicable Executive Order[(1)] and Department of Defense Directive,[(2)] DOHA issued a Statement of Reasons (SOR), detailing the basis for its decision-security concerns raised under Guideline E (Personal Conduct), Guideline K (Security Violations), Guideline D (Sexual Behavior), and Guideline M (Misuse of Information Technology Systems) of the Directive. On June 1, 2005, Applicant submitted an answer to the SOR and elected to have a hearing before an administrative judge. The case was assigned to me July 7, 2003. Applicant waived the fifteen day notification provision of ¶ E3.1.8. of the Directive. (Tr. 5-6; 8-10) On October 7, 2005, I convened a hearing to consider whether it is clearly consistent with the national interest to grant or continue a security clearance for Applicant. The Government called no witnesses and introduced 13 exhibits, which were identified and numbered Ex. 1 through 13. Applicant called one witness and introduced one exhibit, which was identified as Ex. A. All exhibits were admitted to the record without objection. DOHA received the transcript (Tr.) of the proceeding on October 18, 2005.

FINDINGS OF FACT

The SOR in this case contains seven allegations of disqualifying conduct under Guideline E, Personal Conduct; one allegation under Guideline K, Security Violations; four allegations under Guideline D, Sexual Behavior; and one allegation under Guideline M, Misuse of Information Technology Systems. In his answer to the SOR Applicant admitted twelve of the thirteen allegations. He denied as exaggerated the SOR allegation that he had 10 extra-marital affairs while traveling outside of the U.S. on official business from December 1996 to at least June 2004, and that his wife was unaware of five or six of the affairs. Applicant admitted about six or seven extra-marital affairs between December 1996 and at least June 2004, and he told his wife about them when he was preparing his answer to the SOR. (Tr. 63-64.) Applicant's admissions are incorporated as findings of fact.

Applicant is 57 years old. His general area of expertise is electronics, and he is employed by a government contractor to monitor and install security equipment in U.S. embassies. He has held a security clearance since 1968. He served in the Armed Forces for 24 years and was honorably discharged in 1993. (Tr. 109; Ex. A)

Applicant and his wife, a naturalized U.S. citizen, were married in 1981. They are the parents of a child born in 1981. In 1995, Applicant and his wife were divorced. They remarried in 1996. (Exs. 1, 2, 3.)

In 1993, Applicant began working for federal contractors. (Exs. 1, 2, 3.) In 1997, while employed by a federal contractor, he inserted an un-scanned disk into his computer in violation of the policies and procedures of the federal agency to which he had been assigned by his employer. The disk was contaminated with a computer virus. Applicant was verbally reprimanded by his supervisor and issued a letter of caution about his action. He was subsequently transferred to another contract. (Ex. 6; Tr. 28-31.) Applicant defended his conduct by observing that others in his office also failed to scan their disks before inserting them into the Government computers. (Tr. 28-31.)

In March 2000, Applicant was fired from a job (Job 1) for unprofessional conduct in the workplace. Applicant's unprofessional conduct involved two angry verbal outbursts against coworkers and one incident where he purposely knocked a soda can out of a coworker's hand. (Tr. 31-34; Ex. 7; Ex. 8.) The information about Applicant's unprofessional conduct was provided by co-workers and associates. (Ex. 7.) Applicant denied being a hostile person. Applicant's witness was the target of one of his outbursts but said he was not bothered by it. (Ex. 7; Tr. 91; 94-95.)

On about May 1, 2002, Applicant was fired from a job (Job 2) as a contract employee because he used a government computer at the federal agency where he was assigned to access an on-line dating service and arrange a date in a Middle-Eastern country where he was assigned on official government business. Applicant's employer fired him because his dating inquiry telegraphed his travel to and work assignment in the country and had the potential to put him and his coworkers at risk. (Ex. 4, at 1-2; Tr. 50-52.)

After being fired the second time, Applicant sought employment in May 2002 with another government contractor (Job 3). The job he applied for required a security clearance. (Tr. 47.) On his employment application, Applicant failed to list the reasons for his terminations from Job 1 and Job 2. He said he released from Job 2 as the result of "cut backs" and from Job 1 as the result of a "lost contract." (Ex. 13 at 3.) Applicant falsified his job application because he feared he would not get the job if he told the truth. (Tr. 40-41.) He was hired by the government contractor, and, as a new employee, he was provided with the company's policy and procedures regarding sexual harassment complaints. He acknowledged receipt of the company's policy and procedures regarding sexual harassment complaints on June 6, 2002. (Ex. 10.)

In December 2002, while employed at Job 3, Applicant inappropriately touched a female employee, who complained to management. On December 17, 2002, Applicant's employer issued him a letter of warning about his inappropriate behavior. (Ex. 9.)

In 2004, while employed at Job 3, Applicant again used a government computer at his federal work site to access an on-line dating service. He visited the on-line dating service because he saw other employees doing so. His employer learned of this conduct and verbally counseled Applicant and the other employees not to visit dating service sites while at work. (Ex.5 at 3; Tr. 53-55.)

Between December 1996 and June 2004, Applicant's jobs required that he travel outside of the U.S. on official business. He was often assigned to work in foreign countries for several weeks at a time. On June 4, 2004, in a signed, sworn statement made to a special agent of the Defense Security Service, Applicant stated: "Since my wife and I re-married in 1996, I have had about ten extramarital affairs, having sex with other women." (Ex. 5 at 4.) Applicant also stated his wife knew of "about four or five" of the affairs, but he had not told her of the others because he wanted to avoid arguments with her. The extra-marital contacts occurred outside of the U.S. when Applicant was assigned by his employer to official business. He did not inform his security officer of his affairs because he did not think the countries in which they occurred were hostile to the U.S. (Ex 5 at 4.)

In his response to the SOR Applicant did not deny having extra-marital affairs but disputed his earlier statement to the special agent that he had engaged in 10 such affairs. At his hearing he admitted having "about six or seven." (Tr. 63-64.) Some of the women were foreign nationals working in U.S. embassies. Others he met in malls, restaurants, or on the Internet. He still has contact with a woman in a Middle-Eastern country. Since he gave his statement to the special agent in June 2004, Applicant has had a sexual relationship with a woman in an Asian country. She was an employee of a European embassy located in an Asian country. (Tr. 64-77)

On August 9, 2001, Applicant completed a security clearance application (SF-86) as a part of a periodic five-year review of his security worthiness. He signed and certified his answers to the SF-86 as true, complete, and correct. Question 20 on the SF-86 asks whether, in the previous seven years, an applicant has been fired from a job, quit a job

after being told he'd be fired, left a job by mutual consent following allegations of misconduct, left a job by mutual agreement following allegations of unsatisfactory performance, or let a job for another reason under unfavorable circumstances. Applicant responded "no" to Question 20. (Ex. 1.)

On March 31, 2004, Applicant completed and certified as correct a second SF-86. In response to Question 20, Applicant answered "yes" and said he was fired from Job 2 for using a government computer to visit a dating service. Applicant used the on-line dating service to request a female companion to show him around a Middle Eastern country where he been assigned by his employer. Applicant further explained his employer fired him because his solicitation raised security concerns. (Ex. 3) Applicant did not admit he had been fired from Job 1 in March 2000.

POLICIES

"[N]o one has a 'right' to a security clearance." *Department of the Navy v. Egan*, 484 U.S. 518, 528 (1988). As Commander in Chief, the President has "the authority to . . . control access to information bearing on national security and to determine whether an individual is sufficiently trustworthy to occupy a position . . . that will give that person access to such information." *Id.* at 527. The President has restricted eligibility for access to classified information to United States citizens "whose personal and professional history affirmatively indicates loyalty to the United States, strength of character, trustworthiness, honesty, reliability, discretion, and sound judgment, as well as freedom from conflicting allegiances and potential for coercion, and willingness and ability to abide by regulations governing the use, handling, and protection of classified information." Exec. Or. 12968, *Access to Classified Information* § 3.1(b) (Aug. 4, 1995). Eligibility for a security clearance is predicated upon the applicant meeting the security guidelines contained in the Directive.

Enclosure 2 of the Directive sets forth personal security guidelines, as well as the disqualifying conditions and mitigating conditions under each guideline. In evaluating the security worthiness of an applicant, the administrative judge must also assess the adjudicative process factors listed in ¶ 6.3 of the Directive. The decision to deny an individual a security clearance is not necessarily a determination as to the loyalty of the applicant. *See* Exec. Or. 10865 § 7. 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.

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. *See Egan*, 484 U.S. at 531. The Directive presumes a nexus or rational connection between proven conduct under any of the disqualifying conditions listed in the guidelines and an applicant's security suitability. *See* ISCR Case No. 95-0611 at 2 (App. Bd. May 2, 1996).

Once the Government establishes a disqualifying condition by substantial evidence, the burden shifts to the applicant to rebut, explain, extenuate, or mitigate the facts. ISCR Case No. 01-20700 at 3 (App. Bd. Dec. 19, 2002); *see* 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 security clearance." ISCR Case No. 01-20700 at 3.

CONCLUSIONS

Guideline E - Personal Conduct

In the SOR, DOHA alleged under Guideline E that Applicant falsified material facts on a SF-86 he executed on August 9, 2001 when he answered "no" to Question 20 and deliberately failed to disclose he had been fired from a job (¶ 1.a.); that on March 7, 2000, he had been fired from a job for unprofessional behavior in the workplace (¶ 1.b.); that on May 1, 2002, he had been fired from a job for using a government computer to access the Internet to visit a dating service web site, where he gave notice of his assignment to a Middle Eastern country, thereby publicizing his future official government travel and putting his work team at risk (¶ 1.c.); and that he falsified material facts on an employment application on May 21, 2002, when he listed "cut backs" as the reason he was terminated from Job 2 and "lost contract" as the reason he was terminated from Job 1, as described in ¶¶ 1.b. and 1.c. above (¶ 1.d.).

DOHA further alleged under Guideline E that Applicant falsified material facts on the SF-86 he executed March 31, 2004, by responding to Question 20 by answering "yes" and then listing that he had been fired from Job 2 but deliberately failing to disclose he had been fired also from Job 1 (¶1.e.); that he had been verbally counseled in early 2004 for using official U.S. government computers, while on duty, to look at photographs of an on-line dating service (¶ 1.f.); and for the information set forth in ¶¶ 2.a., 3.a., 3.b., and 3.c. of the SOR (¶ 1.g.)

Guideline E conduct raises security concerns because it involves questionable judgment, untrustworthiness, unreliability, lack of candor, dishonesty, or unwillingness to comply with rules and regulations and could indicate that an applicant may not properly safeguard classified information. Directive ¶ E2.A5.l.l.

Applicant's conduct raises security concerns under four Disqualifying Conditions (DC) under Guideline E. First, reliable, unfavorable information about Applicant's unprofessional conduct and questionable judgment was provided by coworkers and associates, raising a concern under DC E2.A5.1.2.1 of the Guideline. Second, Applicant deliberately falsified material facts on two security clearance applications and a job application, raising a security concern under DC E2.A5.1.2.2. of the Guideline. Third, Applicant's inappropriate touching of a female coworker and his multiple, unreported sexual affairs while on official duty overseas raise security concerns under DC E2.A5.1.2.4 of Guideline E because they could make him vulnerable to blackmail and make him vulnerable to coercion, exploitation or duress. Fourth, Applicant's use of the of a government computer, while on official duty, to access an on-line dating service and his failure to follow established policies and procedures for handling secure information stored on computer disks raise

security concerns under DC E2.A5.1.2.5., for they suggest a pattern of dishonesty or rule violations.

Applicant admitted the conduct which gave rise to the Guideline E security concerns identified in the SOR. Through Applicant's own admissions, the Government has established a *prima facie* case that Applicant's Guideline E conduct disqualifies him from being entrusted with classified information.

We turn to an examination of possible Mitigating Conditions (MC) under the Guideline. Because Applicant's coworkers and associates provided information about his unprofessional conduct that was substantiated and pertinent to a determination of his judgment, trustworthiness, or reliability, MC E2.A5.1.3.1 is inapplicable. Neither MC E2.A5.1.3.2. nor MC E2.A5.1.3.3 apply to Applicant's case because his falsifications of his SF-86s and his employment application were recent, not isolated incidents, and were not corrected voluntarily by prompt, good-faith efforts to set the record straight before being confronted with the facts. Applicant asserted he was not candid about being fired from two jobs because he feared he would not be hired if he told the truth. Applicant's reticence to reveal the truth about his conduct suggests that, in some circumstances, he may put his interests before those of the Government. The capacity to be truthful goes to the essence of an individual's security worthiness.

Because Applicant continued the sexual conduct that made him vulnerable to coercion, exploitation, or duress, MC E2.A5.1.3.5. is also inapplicable. None of the other mitigating conditions under Guideline E apply to the facts of Applicant's case. Accordingly, the Guideline E allegations of the SOR are concluded against the Applicant.

Guideline K -Security Violations

In the SOR DOHA alleged under Guideline K of the Directive that Applicant failed to comply with security regulations when he neglected to have a disk scanned before inserting it into his Government computer. The disk was infected with a virus which, in turn, infected his computer on March 6, 1997, in violation of the policy and procedure of the federal agency where he was assigned. Applicant's failure to have the disk scanned resulted in a verbal reprimand from his employer and transfer to another contract (2.a.) Under Guideline K, noncompliance with security regulations raises doubt about an individual's trustworthiness, willingness, and ability to safeguard classified information. E2.A11.1.1.

Applicant's deliberate and negligent conduct raises security concerns under Disqualifying

Condition (DC) E2.A11.1.2.2. of Guideline K. Applicant's conduct was infrequent, making Mitigating condition (MC) E2.A.11.1.3.2 applicable. However, his conduct was deliberate and not the consequence of improper or inadequate training. Thus, MC E2.A11.1.3.1 and E2.A.11.1.3.3 are not applicable. Applicant failed to demonstrate a positive attitude towards the discharge of his security responsibilities. Accordingly, MC E2.A.11.1.3.4. is also inapplicable. The Guideline K allegation of the SOR is concluded against the Applicant.

Guideline D - Sexual Behavior

In the SOR DOHA alleged under Guideline D of the Directive that Applicant touched a female coworker inappropriately on or about December 16, 2002, resulting in a written warning from his employer on December 17, 2002 (¶ 3.a.); that from December 3, 1996, to at least June 4, 2004, and while he was married, Applicant engaged in approximately 10 sexual affairs while traveling on official business outside the U.S; that his wife was unaware of approximately five or six of the affairs and Applicant did not want her to know about them (¶3.b.);.that Applicant did not report any of these extra-marital affairs with foreign nationals to his security officer (¶ 3.c.); and that, as alleged in ¶ 1.f. of the SOR, he was verbally counseled in early 2004 for using official U.S. government computers, while on duty, to look at photos of an on-line dating serviced (¶ 3.d.).

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. E2.A4.1.1. Applicant's conduct raises security concerns under two Disqualifying Conditions (DC) under Guideline D. First, Applicant's public sexual behavior in the workplace raises concerns under DC E2.A4.1.2.4. of Guideline D. In 2002 he touched a female coworker inappropriately and was given a written warning by his employer. Second, in 2004, Applicant used an official Government computer to view photos of an on-line dating service, conduct which resulted in counseling by his employer. This conduct occurred recently, when Applicant was more than 50 years old, and it is not the only indicator of Applicant's questionable judgment and irresponsibility. Accordingly, Mitigating Conditions (MC) E2.A4.1.3.1., E2.A4.1.3.2., and E2.A4.1.3.3. do not apply.

Applicant's several extra-marital affairs took place when he was assigned overseas on official Government business. His liaisons were with foreign nationals, some of whom were employed by embassies abroad. Applicant's wife was not aware of all of his affairs, and it is not clear that she approved of or endorsed her husband's conduct. Additionally, Applicant did not tell his security manager about his sexual contacts with foreign nationals. In 2004, he conducted at least one affair with a foreign national after his interview with a special agent of the Defense Security Service. Applicant's conduct raises security concerns under DC E2.A4.1.2.3. because it caused him to be vulnerable to coercion, exploitation, or duress. None of the mitigating conditions under Guideline D apply to Applicant's disqualifying conduct. Accordingly, the Guideline D allegations of the SOR are concluded against the Applicant.

Guideline M - Misuse of Information Technology Systems

In the SOR, DOHA alleged under Guideline M of the Directive that Applicant's noncompliance with rules, procedures, guidelines or regulations pertaining to information technology systems, as alleged in ¶¶ 1.c., 1.f., and 2.a. of the SOR, raised security concerns about his trustworthiness, willingness, and ability to properly protect classified systems, networks, and information (¶ 4.a.).

In 1997, Applicant failed to comply with the policy and procedures at the Government agency where he was assigned. He put an unapproved disk in a Government computer, causing the computer to become infected with a virus. In 2002, Applicant was fired from a job requiring a security clearance when he used the Internet, in advance of official travel to the Middle East, to solicit female companionship, thus publicizing his travel and jeopardizing the security of his travel team and coworkers. In 2004, Applicant was verbally counseled for using an official Government computer to access the Internet to look at photos of an on-line dating service.

Applicant's two unauthorized entries into official Government technology systems in 2002 and 2004 and his 1997 unauthorized introduction of an unscanned and infected software disk into a Government computer, in violation of agency policy and procedures, raise security concerns under Disqualifying Conditions (DC) E2.A.13.1.2.1. and E2.A.13.1.2.4. of Guideline M. Applicant's misuse of Government technology systems was recent and significant. His conduct was intentional, and his introduction of infected software was not authorized. His misuse of information technology systems was not limited to an isolated event, nor was it followed by a prompt, good faith effort to correct the situation. Accordingly, Mitigating Conditions (MC) E2.A.13.1.3.1, E2.A.13.1.3.2., E2.A13.1.3.3., E2.A.13.1.3.4., and E2.A.13.1.3.5. do not Apply to the facts of Applicant's case, and the Guideline M allegations of the SOR are concluded against the Applicant.

In my evaluation of the record, I have carefully considered each piece of evidence in the context of the totality of evidence and under all of the Directive guidelines that were generally applicable or might be applicable to the facts of this case. Under the whole person concept, I conclude that Applicant has not successfully overcome the Government's case opposing his request for a DoD security clearance.

FORMAL FINDINGS

The following are my conclusions as to the allegations in the SOR:

Paragraph 1. Guideline E: AGAINST APPLICANT

Subparagraph 1.a.: Against Applicant

Subparagraph 1.b.: Against Applicant

Subparagraph 1.c.: Against Applicant

Subparagraph 1.d.: Against Applicant

Subparagraph 1.e.: Against Applicant

Subparagraph 1.f.: Against Applicant

Subparagraph 1.g.: Against Applicant

Paragraph 2. Guideline K: AGAINST APPLICANT

Subparagraph 2.a.: Against Applicant

Paragraph 3. Guideline D: AGAINST APPLICANT

Subparagraph 3.a.: Against Applicant

Subparagraph 3.b.: Against Applicant

Subparagraph 3.c.: Against Applicant

Subparagraph 3.d.: Against Applicant

Paragraph 4. Guideline M: AGAINST APPLICANT

Subparagraph 4.a.: Against Applicant

DECISION

In light of all of 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.

Joan Caton Anthony

Administrative Judge

1. Exec. Or. 10865, *Safeguarding Classified Information within Industry* (Feb. 20, 1960), as amended and modified.

2. Department of Defense Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (Jan. 2, 1992), as amended and modified.