KEYWORD: Information Technology; Personal Conduct

DIGEST: Applicant has been employed by federal contractors since his retirement from the Navy. His retirement was by mutual agreement with his commander based upon Applicant's admissions at the time he had used his government computer against regulations, and had shared inappropriate information he obtained through his computer with coworkers while on duty. Applicant failed to disclose the reason for his retirement on two separate Security Clearance Applications (SF 86) he submitted in 2000 and 2003. Applicant failed to mitigate the security concerns regarding his misuse of government technology systems and personal conduct. Clearance is denied.

CASENO: 04-03735.h1

DATE: 10/27/2005

DATE: October 27, 2005

In re:

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

Applicant for Security Clearance

ISCR Case No. 04-03735

DECISION OF ADMINISTRATIVE JUDGE

DAVID S. BRUCE

APPEARANCES

FOR GOVERNMENT

Raymond T. Blank, Jr., Esq., Department Counsel

FOR APPLICANT

Pro Se

SYNOPSIS

Applicant has been employed by federal contractors since his retirement from the Navy. His retirement was by mutual agreement with his commander based upon Applicant's admissions at the time he had used his government computer against regulations, and had shared inappropriate information he obtained through his computer with coworkers while on duty. Applicant failed to disclose the reason for his retirement on two separate Security Clearance Applications (SF 86) he submitted in 2000 and 2003. Applicant failed to mitigate the security concerns regarding his misuse of government technology systems and personal conduct. Clearance is denied.

STATEMENT OF THE CASE

On April 8, 2005, the Defense Office of Hearings and Appeals (DOHA), pursuant to Executive Order 10865, *Safeguarding Classified Information Within Industry,* dated February 20, 1960, as amended and modified, and Department of Defense Directive 5220.6, *Defense Industrial Review Program,* dated January 2, 1992, as amended and modified (Directive), issued a Statement of Reasons (SOR) to Applicant alleging facts that raise security concerns addressed in the Directive under Guideline M - Misuse of Information Technology Systems, and Guideline E - Personal Conduct. The SOR detailed why DOHA could not preliminarily determine under the Directive that it is clearly consistent with the national interest to grant or continue Applicant's request for a security clearance. By his answer executed May 25, 2005, Applicant admitted the allegations of subparagraphs 1.a. and 2.a. through 2.c. of the SOR, and submitted a letter with his answer explaining his admissions. He also requested a hearing before an administrative judge.

The case was assigned to me on August 24, 2005, and I conducted the hearing on September 20, 2005. The government submitted exhibits (GE) 1 through 4, which were admitted without objection. Applicant testified at the hearing and offered no documentary evidence. DOHA received the hearing transcript (Tr.) on September 28, 2005.

FINDINGS OF FACT

Applicant is 44 years old and has been employed by a defense contractor as an engineer technician since October 2002. He was previously employed by other federal contractors since he retired from the Navy in September 2000.[(1)] He served over 21 years in the Navy and retired at the paygrade of E-8, and was honorably discharged.[(2)]

In November and December 1999, Applicant and others under his command shared information they received on government computers from pornographic web sites and other sources. As a result, Applicant was given the option by his commander to retire or face Captain's Mast proceedings concerning his conduct.[(3)] Applicant chose to retire and was transferred to another duty station until his discharge.[(4)] In accordance with Applicant's agreement with his commander, there was no record made in Applicant's personnel file regarding the reason for his 'early' retirement.[(5)]

When the computer incidents occurred in 1999, Applicant was taking college courses in the evening and was authorized to use his government computer during evening hours to do schoolwork. Some of the inappropriate information and materials captured on his computer was generated when he was using the computer for personal use, and sometimes sent to him by others.[(6)]

In response to Question 20, **Your Employment Record,** on Applicant's Security Clearance Applications (SF 86), dated December 11, 2000, and April 16, 2003, Applicant answered "No" when asked whether he had ever left a job by mutual agreement or any other reason under unfavorable circumstances in the preceding 10 year period.[(7)]

Applicant has not been charged with a criminal offense in the past 7 years and has been responsible with his personal financial affairs.[(8)] He does not use illegal drugs or abuse alcohol, and he previously held a secret clearance in 1995 when he was in the Navy.[(9)]

POLICIES

Enclosure 2 of the Directive, *Adjudicative Guidelines For Determining Eligibility For Access To Classified Information,* sets forth the criteria which must be evaluated when determining security clearance eligibility. The adjudicative guidelines specifically distinguish between those factors that are considered in denying or revoking an employee's request for access to classified information (Disqualifying Conditions), together with those factors that are considered in granting an employee's request for access to classified information (Mitigating Conditions). By acknowledging that individual circumstances of each case are always different, the guidelines provide substantive standards to assist an administrative judge in reaching fair and impartial common sense decisions.

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 well- informed decisions. 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 conduct of the applicant and the circumstances in any case, the factors an administrative judge should consider pursuant to the concept are: (1) the nature, extent, and seriousness of the conduct; (2) the circumstances surrounding the conduct, to include knowledgeable participation; (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 the participation; (6) the presence or absence of rehabilitation and other pertinent 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.

Protecting national security is the paramount concern in reaching a decision in any case, and is dependent upon the primary standard that issuance of a clearance must be clearly consistent with the interests of national security. Granting an applicant's clearance for access to classified information is predicated on a high degree of trust and confidence in the individual. Accordingly, decisions under the Directive must include consideration of not just the *actual* risk of disclosure of such information, but also consideration of any *possible* risk an applicant may deliberately or inadvertently compromise classified information in any aspect of his or her life. Any doubt about whether an applicant should be allowed access to classified information must be resolved in favor of protecting classified information.[(10)] The decision to deny a security clearance request to an individual is not necessarily a determination of the loyalty of the applicant.[(11)] It is merely an indication the applicant has not met the strict guidelines established by the Department of Defense for issuing a clearance.

In accordance with the Directive, the government bears the burden of proof in the adjudicative process to first establish conditions by substantial evidence which indicate it is not clearly consistent with the national interest to grant or continue an applicant's access to classified information.[(12)] The legal standard for the burden of proof is something less than a preponderance of the evidence.[(13)] When the government meets this burden, the corresponding heavy burden of rebuttal then falls on the applicant to present evidence in refutation, explanation, extenuation or mitigation sufficient to overcome the position of the government, and to ultimately demonstrate it is clearly consistent with the national interest to grant or continue the applicant's clearance.[(14)]

Upon consideration of all the evidence submitted in this matter, the following adjudicative guidelines are appropriate for evaluation with regard to the facts of this case:

Guideline M - 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.

Guideline E - Personal conduct is a security concern because conduct involving questionable judgment, trustworthiness, unreliability, lack of candor, dishonesty, or unwillingness to comply with rules and regulations could indicate that the person may not properly safeguard classified information.

CONCLUSIONS

I have thoroughly considered all the facts in evidence in this case and the legal standards required by the Directive. The government has established a *prima facie* case for disqualification under Guideline M - Misuse of Information Technology Systems.

Based upon all the evidence, Misuse of Information Technology Systems Disqualifying Condition (MITS 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)* and MITS DC E2.A13.1.2.4. *(Introduction of hardware, software or media into any information technology system without authorization, when specifically prohibited by the rules, procedures, guidelines or regulations),* apply in this case. Applicant admits he accessed pornographic web sites on his government computer in 1999 while serving in the U.S. Navy, and sharing inappropriate, sexually oriented materials with others under his supervision while on duty. The governments's evidence and Applicant's admissions constitute substantial evidence of behavior that qualifies as serious conduct within the meaning of Guideline M.

I have considered all the Misuse of Information Technology Systems Mitigating Conditions (MITS MC) and, specifically, MITS MC E2.A13.1.3.1. *(The misuse was not recent or significant),* and MITS MC E2.A13.1.3.4. *(The misuse was an isolated event).* I conclude none apply in this case.

When a person is entrusted with sensitive or classified information in the performance of their job responsibilities, the individual must be reliable and capable of safeguarding the information whether in the workplace or outside the employment environment. When an individual is unwilling or unable to comply with rules, procedures, and regulations pertaining to information technology, security concerns are raised about that individual's trustworthiness, willingness,

and conscientious ability to properly protect classified networks and related information. Applicant's use of his government computer in accessing pornographic materials was exacerbated by him sharing such materials with coworkers, and then forwarding it to others. As such, the conduct cannot be considered an insignificant or isolated event. He viewed, stored, and shared inappropriate material with a number of subordinates over an unknown period of time. Nor was his conduct unintentional or inadvertent. He knew what kind of material was involved, and that his actions were against government regulations. Nonetheless, he persisted in the conduct over time, continuing to involve subordinates under his leadership. He did not endeavor to discontinue his or his coworkers' conduct, but actually perpetuated the inappropriate behavior by involving both male and female subordinates under his supervision.

I have further considered all the facts in evidence set forth above and conclude the government has also established its case for disqualification under Guideline E - Personal Conduct. Based on all the evidence, Personal Conduct Disqualifying Condition (PC DC) E2.A5.1.2.2. *(The deliberate omission, concealment, or falsification of relevant and material facts from any personnel security questionnaire, personal history statement, or similar form used to conduct investigations, determine employment qualifications, award benefits or status, determine security clearance eligibility or trustworthiness, or award fiduciary responsibilities)* and 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 knowingly and willfully violated Navy regulations regarding the use of his government computer. Such behavior qualifies as prohibitive conduct under Guideline E, particularly when perpetrated in a military setting by a senior noncommissioned officer. He also failed to disclose material information requested on his SF 86.

I have considered all the Personal Conduct Mitigating Conditions (PC MC), and specifically, PC MC E2.A5.1.3.3. *(The individual made prompt, good faith efforts to correct the falsification before being confronted with the facts),* and find none apply.

Applicant's commander afforded him the opportunity to retire from the Navy rather than face criminal charges for misconduct. He elected to retire, upon evaluating his personal circumstances at the time, and further predicated on the understanding no record of the matter would be retained in his permanent personnel file. Applicant failed to disclose the actual circumstances of his retirement from the Navy when he answered Question 20 on his SF 86 dated December 11, 2000, and again on another SF 86 he submitted in April 2003. Applicant's obligation to provide complete and honest answers on an SF 86 application was not diminished by the terms of an agreement he may have had with his Navy commander. The question is clear when asked to disclose any reason for having left employment - "by mutual agreement following allegations of misconduct...unsatisfactory performance...[or]...unfavorable conditions."[(15)] While it is true the circumstances leading up to his retirement were not reflected in his personnel record, his answer on his December 2000 application was still misleading. It was not based on the true facts known to him at the time, and Applicant underestimated the resourcefulness of the Defense Security Service. A reasonable inference can be drawn that Applicant's answer was logically calculated to inappropriately influence the outcome of his clearance request. He then had over two years to reconsider his answer and correct the misstatement when he submitted his second application, yet he made no attempt to do so before being confronted with the misinformation. The gravity of Applicant's conduct in this regard creates serious doubt about Applicant's judgment, reliability and trustworthiness, and, accordingly, he has failed to successfully mitigate the security concerns raised under Guideline E.

I have considered the record evidence in this case including Applicant's credibility and demeanor and the "whole

person" concept required by the Directive in evaluating Applicant's risk and vulnerability in protecting our national security. Although Applicant's loyalty to the United States is not in question, I am persuaded by the totality of the evidence it is not clearly consistent with the national interest to grant Applicant a security clearance. For the reasons stated, Applicant has failed to mitigate the security concerns raised by his misuse of information technology systems and personal conduct. Accordingly, Guideline M and Guideline E are decided against Applicant.

FORMAL FINDINGS

In accordance with Section E3.1.25 of Enclosure 3 of the Directive, the following are the formal findings as to each allegation in the SOR:

Paragraph 1. Misuse of Information Technology Systems (Guideline M) AGAINST THE APPLICANT

Subparagraph 1.a. Against the Applicant

Paragraph 2. Personal Conduct (Guideline E) AGAINST THE APPLICANT

Subparagraph 2.a. Against the Applicant

Subparagraph 2.b. Against the Applicant

Subparagraph 2.c. Against 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.

David S. Bruce

Administrative Judge

1. GE 4 (Applicant's Security Clearance Application dated April 16, 2003), at 2-4.

2. *Id.,* at 6-7.

3. Tr., at 30-38.

4. GE 2 (Applicant's statement to Defense Security Service Special Agent dated June 24, 2003), at 3. See also Tr., at 46 and 49.

5. Tr., at 16 and 38-39.

6. GE 2, *supra* note 4, at 2.

7. GE 1 (Applicant's Security Clearance Application dated December 11, 2000), at 8; and, GE 4, *supra* note 1, at 6-7.

8. GE 4, *supra* note 1, at 7-9.

9. *Id.,* at 9.

10. Directive, Enclosure 2, Para. E2.2.2.

11. Executive Order 10865 § 7.

12. ISCR Case No. 96-0277 (July 11, 1007) at p. 2.

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

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

15. GE 1, *supra* note 7, at 6-7, and GE 4, *supra* note 1, at 8.