KEYWORD: Personal Conduct; Misuse of Information System Technologies

DIGEST: Applicant is a 47-year-old employee of a defense contractor. While working for his former employer between 1996 and 2002, Applicant accessed inappropriate material on the internet. The prohibited practice continued despite oral and written warnings by his superiors. He no longer accesses such material in the work place. Applicant has mitigated concerns regarding the misuse of information system technologies, but has failed to allay concerns arising from his repeated violations of company policy and rules. Applicant has failed to mitigate the personal conduct concerns raised. Clearance is denied.

CASE NO: 05-01308.h1

DATE: 05/26/2006

DATE: May 26, 2006

In re:

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

Applicant for Security Clearance

ISCR Case No. 05-01308

DECISION OF ADMINISTRATIVE JUDGE

ARTHUR E. MARSHALL, JR.

APPEARANCES

FOR GOVERNMENT

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

FOR APPLICANT

Pro se

SYNOPSIS

Applicant is a 47-year-old employee of a defense contractor. While working for his former employer between 1996 and 2002, Applicant accessed inappropriate material on the internet. The prohibited practice continued despite oral and written warnings by his superiors. He no longer accesses such material in the work place. Applicant has mitigated concerns regarding the misuse of information system technologies, but has failed to allay concerns arising from his repeated violations of company policy and rules. Applicant has failed to mitigate the personal conduct concerns raised. Clearance is denied.

STATEMENT OF THE CASE

On September 22, 2005, the Defense Office of Hearings and Appeals (DOHA) issued to Applicant a Statements of Reasons (SOR) concluding it was 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, alleged security concerns under Guideline M (Misuse of Information Technology Systems) and Guideline E (Personal Conduct). In a notarized letter, dated October 12, 2005, Applicant responded to the SOR allegations[(2)] and waived his right to an administrative hearing in favor of a decision based on the record.

Department Counsel prepared a File of Relevant Material (FORM) which was mailed to Applicant on March 7, 2006. He acknowledged receipt of the FORM on March 17, 2006, and has declined to object to the information contained in the FORM or to supply additional information for consideration. The case was assigned to me on May 17, 2006.

FINDINGS OF FACT

Applicant's admission to the allegation in paragraph one of the SOR,[(3)] is incorporated herein. After a thorough and careful review of the pleadings, exhibits, and testimony, I make the following findings of fact:

Applicant is a 47-year-old employee of a defense contractor. He is married and has four preteen children. He attended a four-year university, but does not hold a formal degree. Applicant worked for other defense contractors and was previously granted a Department of Defense security clearance in 1998.

From August 1996 through October 2002, Applicant worked for a defense contractor as a cryptographic engineer. During that term of employment, he accessed pornographic and other prohibited web sites on his work computer. Such personal use was against company policy and the rules set forth in the employee handbook.[(4)] Those incidents resulted in oral warnings by both his supervisor and the facility security officer for "constantly (accessing) inappropriate sites on the Internet."[(5)]

Applicant subsequently sent an e-mail that was deemed by his superiors as "offensive, inappropriate, and (in violation of the company's) Standards of Conduct and Sexual Harassment policies."[(6)] On August 12, 2002, that action resulted in a written warning from the company's human resources manager, who elevated the issue to the next step in the company's disciplinary process. Approximately two weeks later, the chairman of the company wrote Applicant to inform him that his continued employment by the company was in "serious jeopardy."[(7)] It was noted that Applicant had continued performing "inappropriate activity after the company issued a written policy prohibiting such activity."[(8)] The chairman's letter concluded by noting: "[C]onsider this letter a warning that any continued activity of this sort will result in immediate termination without further notice."[(9)]

Counseling about Applicant's misuse of the company's computer and access of inappropriate material and web sites was provided during this period by his boss, his security officer, and human resources personnel.[(10)] Despite counseling, Applicant continued to access pornographic material of varied content and occasionally triggered pop-ups of unforseen content. Sometimes this material would arise from otherwise benign origins on the internet.[(11)]

In October 2002, Applicant was released from his employment. He was told that his severance was due to economic reasons.[(12)] He then entered into a period of unemployment that lasted from November 2002 through at least March 2005, when he completed his security clearance application. Knowledge of the incidents regarding inappropriate internet access is not widely known, but he does not care if anyone knows about them. His wife knows about the conduct at issue.[(13)]

Consequently, he does not feel that this information can be used against him for coercive purposes. He states he has not accessed similar material in subsequent employment and there is no evidence of record indicating that he has. He has been at his new job for approximately a year.[(14)]

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. 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.(15) The government has the burden of proving controverted facts.(16) The burden of proof is something less than a preponderance of evidence.(17) 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.(18) Additionally, an applicant has the ultimate burden of persuasion to obtain a favorable clearance decision.(19)

No one has a right to a security clearance(20) and "the clearly consistent standard indicates that security clearance determinations should err, if they must, on the side of denials."(21) Any reasonable doubt about whether an applicant should be allowed access to sensitive information must be resolved in favor of protecting such sensitive information.(22) The decision to deny an individual a security clearance is not necessarily a determination as to the loyalty of an applicant.(23) 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 M - Misuse of Information Technology Systems. *The Concern*: Noncompliance with rules, procedures, guidelines of 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, mission, processing, manipulation, and storage of classified information.[(24)]

Guideline E - Personal Conduct. *The Concern*: 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.[(25)]

Conditions pertaining to these adjudicative guidelines that could raise a security concern and may be disqualifying, as well as those which would mitigate security concerns, 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 M (Misuse of Information Technology Systems) and under Guideline E (Personal Conduct). For clarity, I will discuss those guidelines separately.

Misuse of Information Technology Systems

Applicant used property of his defense contractor employer to access inappropriate and pornographic material on the internet. Such activity continued despite warnings and counseling on the matter. He was on notice of the company's position regarding the use of technology resources by the applicable sections in the employee handbook. He was advised that such activity was in violation of the company's Standards of Conduct and Sexual Harassment policies. It

was particularly noted by the company's chairman that Applicant had continued to access inappropriate and pornographic material through corporate property even after the company had specifically issued a written policy prohibiting such activity. Such behavior gives rise to Misuse of Information Technology Systems Disqualifying Condition (MIT DC) E2.A13.1.2.1([*i*]*llegal or unauthorized entry into any information technology system*).

The Guideline also sets forth certain mitigating conditions that may be raised to mitigate or explain the conduct at issue. Here, the conduct occurred prior to Applicant's severance from his former employment in October 2002. Although exact dates for the incidents at issue are unknown, he began working with the company in August 1996 and the last reported incident noted in the FORM occurred sometime prior to August 12, 2002. Moreover, there is no indication that this behavior has continued in his present employment situation. Given that nearly four years have passed since the last noted incident of misuse, Misuse of Information Technology Systems Mitigating Condition (MIT MC) E2.A13.1.3.1 ([*t*]*he misuse was not recent or significant*) applies.

In his statements, Applicant notes that some of his access to inappropriate material was inadvertent and that some took the shape of pop-ups, over which he had no control. This is credible to the extent that web content catering to prurient interests has metastasized throughout the internet since its introduction to the public. Moreover, pop-ups of licentious content are notorious for self-multiplication from otherwise benign looking sites. Because some of the material accessed by Applicant was done so inadvertently, MIT MC E2.A13.1.3.2 ([*t*]*he conduct was unintentional or inadvertent*) applies, but only to a limited extent. None of the other mitigating conditions, however, apply.

Personal Conduct

During the Applicant's security investigation, it was discovered that he had used his former employer's computer to access inappropriate material, that he had been counseled as to the activity, and that he had been warned both orally and in writing with regard to that activity. Both the counseling and the warnings reenforced the policies set forth in the employee handbook. Consequently, Personal Conduct Disqualifying Condition (PC DC) E2.A5.1.2.1 ([*r*]*eliable, unfavorable information provided by associates, employers, coworkers, neighbors, and other acquaintances*) 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.

The Government asserts that Applicant's wife does not know about the incidents at issue and that he does not want her to know about them. This allegation is allegedly based on a statement by a superior at Applicant's former workplace that Applicant told him or her that was the case. The Government, however, did not introduce into the record a copy of any correspondence, statement, or investigative report from which this hearsay is based. As such, the allegation is unsubstantiated. Regardless, Applicant denies ever making such a statement to a superior and denies the allegation. Because the Government failed to prove the fact alleged at the onset, and given Applicant's flat denial that the allegation is untrue, I find the pertinent SOR allegation, subparagraph 2.a, in Applicant's favor.

The Government's remaining allegation regarding personal conduct is that Applicant's misuse of information technology systems gives rise to personal conduct issues. Applicant admits that he continued to access inappropriate material despite the fact it was against known policies and rules. He also acknowledges that his misuse continued despite repeated warnings, oral and written, from superiors. In view of the personal conduct mitigating conditions available under Guideline E, none of those mitigating conditions apply.

I have reviewed the record as a whole and considered Applicant under the "whole person" concept, Applicant is a mature professional man with a wife and children at home. Whether he accessed inappropriate and pornographic material because he thought it was salacious, funny, harmless, or a way to pass the time is unknown. What is known is that he was forewarned of his company's position as to the use of its technology systems, was counseled with regard to both the inappropriateness of his activities and to their contravention of the workplace's rules and policies, and was disciplined for his repeated violations.

The passage of nearly four years since his last documented incident and his current abstinence from such activity in the workplace marginally mitigates concerns regarding Applicant's misuse of information technology systems. His repeated and flagrant actions, however, demonstrate both questionable judgment and an unwillingness to comply with rules and regulations; his inability to comport his behavior after both counseling and disciplinary action raises genuine concerns regarding his trustworthiness and reliability. Given these circumstances, I find that Applicant has failed to mitigate security concerns arising under Guideline E (Personal Conduct). Clearance is denied.

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 M (Misuse of Information FOR APPLICANT

Technology Systems)

Subparagraph 1.a: For Applicant

Paragraph 2. Guideline E (Personal Conduct) AGAINST APPLICANT

Subparagraph 2.a: Against Applicant

Subparagraph 2.b: For Applicant

DECISION

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

_____

Arthur E. Marshall, Jr.

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. Applicant admitted to the allegation raised under Guideline M, but denied those raised under Guideline E.

3. Applicant admits the conduct underlying SOR subparagraph 2.a, which is the same conduct admitted to under paragraph 1; he denies, however, the allegation set forth in subparagraph 2.b.

4. Government Item 5 (Employee Handbook excerpt).

5. Government Item 7 (Chairman's Warning Letter, dated August 25, 2005).

6. Government Item 8 (Written Warning/Memorandum to Applicant from Employer, dated August 12, 2002).

7. Government Item 7, *supra*, footnote 2.

8. *Id.*

9. *Id.*

10. Government Item 6 (Applicant's Statement to a Contract Investigator of the Defense Security Service, dated July 15, 2003).

11. *Id.*

12. *Id.* The Government suggests that Applicant was let go due to his access of inappropriate material on the internet, but there is no documentation supporting that suggestion. Indeed, Applicant's assertion that others were let go at the same time for financial reasons is plausible given the year and the industry, and it is not contradicted by the other facts in the record.

13. The Government does not proffer any documentation showing that Applicant's wife was shielded from these facts. Instead, it apparently relies on a statement by a former superior that is not contained in the record. Applicant denies discussing his wife with his former superior and states that his wife is aware of the conduct at issue. His assertion is not contradicted by materials in the FORM and the Government did not proffer any supporting evidence when it made its rebuttal. *See* Government Item 3 (Applicant's Answer to the SOR, dated October 12, 2005) and Government Item 6, *supra*, footnote 6.

14. Item 3, *supra*, footnote 12. Applicant was still unemployed when he completed his security clearance application on March 23, 2005. Assuming he was hired shortly thereafter, Applicant has been employed with his current employer, at most, for a little over a year.

15. ISCR Case No. 96-0277 at 2 (App. Bd. Jul 11, 1997).

16. ISCR Case No. 97-0016 at 3 (App. Bd. Dec 31, 1997); Directive, Enclosure 3, ¶ E3.1.14.

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

18. ISCR Case No. 94-1075 at 3-4 (App. Bd. Aug 10, 1995); Directive, Enclosure 3, ¶ E3.1.15.

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

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

21. *Id*.

22. *Id*.; Directive, Enclosure 2, ¶ E2.2.2.

23. Executive Order 10865 § 7.

24. Directive, Enclosure 2, ¶ E2.A13.1.1.

25. Directive, Enclosure 2, ¶ E2.A5.1.1.