**DEPARTMENT OF DEFENSE**
**DEFENSE OFFICE OF HEARINGS AND APPEALS**

| | | |
|---|---|---|
| In the matter of: | ) | |
| | ) | |
| ---------- | ) | ISCR Case No. 07-00819 |
| SSN: ---------- | ) | |
| | ) | |
| Applicant for Security Clearance | ) | |

**Appearances**

For Government: James F. Duffy, Esquire, Department Counsel
For Applicant: *Pro Se*

June 23, 2008

**Decision**

MATCHINSKI, Elizabeth M., Administrative Judge:

Applicant submitted an Electronic Questionnaire for Investigations Processing (e-QIP) on August 17, 2005. On October 30, 2007, the Defense Office of Hearings and Appeals (DOHA) issued a Statement of Reasons (SOR) to Applicant detailing security concerns under Guideline M and Guideline E as the bases for its decision to deny his request for a security clearance. The action was taken under Executive Order 10865, *Safeguarding Classified Information within Industry* (February 20, 1960), as amended; Department of Defense Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (January 2, 1992), as amended (Directive); and the revised adjudicative guidelines (AG) promulgated by the President on December 29, 2005, and effective within the Department of Defense for SORs issued after September 1, 2006.

Applicant answered the SOR in writing on November 16, 2007, and requested a decision without a hearing. On February 27, 2008, the government submitted a File of Relevant Material (FORM) consisting of nine exhibits (Items 1-9). DOHA forwarded a copy of the FORM to Applicant and instructed him to respond within 30 days of receipt. Applicant submitted no response by the April 6, 2008, deadline. On May 27, 2008, the

case was assigned to me to consider whether it is clearly consistent with the national interest to grant or continue a security clearance for Applicant. Based upon a review of the government's FORM, including Applicant's Answer to the SOR allegations (Item 4), eligibility for access to classified information is denied.

## Findings of Fact

DOHA alleged under Guideline M, use of information technology systems, and Guideline E, personal conduct, that Applicant was terminated by a former employer in January 2005 for using his government-provided computer and Internet access to view sexually explicit prohibited web sites in violation of government policies (SOR ¶¶ 1.a and 2.a). Applicant admitted that while employed as a systems administrator, he surfed the Internet, and viewed pornographic web sites. He apologized for his "terrible mistake" and averred it would not be repeated (Item 4). After reviewing the available evidence, I make the following findings of fact:

Applicant is a 48-year-old designer who has been employed by a division of a large defense contractor since March 2005. He had worked for the company as an engineering analyst from July 1982 to June 2000 before it was acquired by its present corporate parent. During his previous tenure, Applicant had collateral duties as the security representative for his section (Item 4, Item 5). His present position occasionally requires access to areas where a security clearance is required (Item 4).

Applicant was married to his first wife from June 1980 to April 1991. They had twin daughters born in June 1981. He was on active duty in the U.S. military from July 1978 to July 1982 and held a top secret-level clearance. After his four-year enlistment ended, he began working for his present employer as an engineering analyst. He produced and updated drawings that were classified in nature (Item 4, Item 5).

In late June 1991, Applicant married his current spouse and became a stepfather to two children aged 14 and 11. In June 2000, he left his defense contractor position for the information technology sector. He worked for a succession of companies gaining experience and responsibility (Item 4, Item 5).

From September 2001 to January 2005, he was employed as a contract computer systems administrator on a government installation. Applicant was responsible for administering a computer network connected to other federal installations and he had daily access to a secure government computer. He also had a second government computer with electronic mail and Internet access capability that he used daily in the performance of his non-classified work. On October 3, 2002, Applicant signed an Automated Information Systems User Acknowledgment Form authorizing his use of a government-owned computer solely for business purposes (Item 4, Item 6, Item 7).

Secure transmissions took 30 minutes or more to complete and Applicant found himself with substantial "down time" on the job. In about early 2004, Applicant began to

surf the Internet using his non-secure computer while awaiting secure transmissions. He accessed several different types of non-business related web sites, including sport, government and politics, finance and investment, news, photo searches, arts and entertainment, education, personals and dating, travel, and even hate speech. At times, he spent up to three hours in a given workday accessing the Internet for personal purposes. Applicant considered the secure computer network to be his prime responsibility, and as long as it was being monitored and running smoothly, he was doing his job (Item 6, Item 7).

Between October 5, 2004, and December 23, 2004, Applicant spent about 7.95 total hours accessing over 500 sexually explicit prohibited web addresses on his government work computer (Item 7). Applicant was aware access to pornography was prohibited by government policy and in violation of the Automated Information Systems Acknowledgment Form he had executed in October 2002, but he thought it was no big deal since his work was being done (Item 6). On January 12, 2005, the government contracting officer directed Applicant's employer to remove him from his position on the federal installation and terminate his services under the contract immediately because of his unauthorized Internet access to sexually explicit prohibited web addresses, in violation of the service's core values of honor, respect, and devotion to duty, the policies and guidelines involving personal use of government office equipment, and the agreement Applicant had signed limiting his access to business purposes (Item 7). When confronted by his employer, Applicant admitted his mistake. He was terminated from his job for cause (Item 6).

Applicant was out of work for a few months until March 2005, when he was hired by his present employer. Needing a security clearance for his work as a designer, Applicant completed an e-QIP on August 17, 2005. He responded "Yes" to question 22, concerning whether he had been fired from, quit, or left a job within the past seven years under adverse circumstances, and indicated that in January 2005, he had "Left a job for other reasons under unfavorable circumstances. Internet Misuse." (Item 5).

On October 5, 2006, Applicant was interviewed by an investigator for the Department of Defense about his separation from his previous employment. Applicant indicated he had used his non-secure computer solely for business until the last nine to twelve months of his employment when he began to surf the Internet during down time in his job. Applicant explained his initial access to pornography using his work computer was unintended (he entered an "innocent search word" into the Google search engine and a porn site popped up) but he found them interesting and began looking at some of them out of curiosity. Applicant admitted he knew he should not have been surfing the Internet, particularly adult web sites. He did not consider it a big deal since his work was being done. When he was called in by the company's president, Applicant thought he was going to be warned or reprimanded but he was fired. Applicant admitted he was not allowed to collect unemployment even though he also claimed the president indicated he would tell anyone who called that he had been laid off. Applicant denied he had a big interest in pornography and indicated to the investigator he had made a "stupid

decision" to access the adult sites and had learned his lesson. Applicant averred that his spouse and his boss know about the details of the job termination (Item 6).

As of May 2007, Applicant's spouse was also working as a designer for the defense contractor that employs Applicant (Item 6). Applicant denies he could be subjected to blackmail or coercion. To his understanding, he was fired for "excessive unauthorized internet abuse." In Answer to the SOR, Applicant expressed his remorse and vowed to not repeat it ("I admit that I made a terrible mistake and apologize for it and will not repeat it in the future.") (Item 4).

## Policies

When evaluating an applicant's suitability for a security clearance, the administrative judge must consider the revised adjudicative guidelines (AG). In addition to brief introductory explanations for each guideline, the adjudicative guidelines list potentially disqualifying conditions and mitigating conditions, which are useful in evaluating an applicant's eligibility for access to classified information.

These guidelines are not inflexible rules of law. Instead, recognizing the complexities of human behavior, these guidelines are applied in conjunction with the factors listed in the adjudicative process. The administrative judge's overarching adjudicative goal is a fair, impartial and common sense decision. According to AG ¶ 2(c), the entire process is a conscientious scrutiny of a number of variables known as the "whole person concept." The administrative judge must consider all available, reliable information about the person, past and present, favorable and unfavorable, in making a decision.

The protection of the national security is the paramount consideration. AG ¶ 2(b) requires that "[a]ny doubt concerning personnel being considered for access to classified information will be resolved in favor of national security." In reaching this decision, I have drawn only those conclusions that are reasonable, logical and based on the evidence contained in the record. Likewise, I have avoided drawing inferences grounded on mere speculation or conjecture.

Under Directive ¶ E3.1.14, the government must present evidence to establish controverted facts alleged in the SOR. Under Directive ¶ E3.1.15, the Applicant is responsible for presenting "witnesses and other evidence to rebut, explain, extenuate, or mitigate facts admitted by applicant or proven by Department Counsel. . . ." The Applicant has the ultimate burden of persuasion as to obtaining a favorable security decision.

A person who seeks access to classified information enters into a fiduciary relationship with the government predicated upon trust and confidence. This relationship transcends normal duty hours and endures throughout off-duty hours. The government reposes a high degree of trust and confidence in individuals to whom it grants access to classified information. Decisions include, by necessity, consideration of the possible risk

the Applicant may deliberately or inadvertently fail to protect or safeguard classified information. Such decisions entail a certain degree of legally permissible extrapolation as to potential, rather than actual, risk of compromise of classified information.

Section 7 of Executive Order 10865 provides that decisions shall be "in terms of the national interest and shall in no sense be a determination as to the loyalty of the applicant concerned." *See also* EO 12968, Section 3.1(b) (listing multiple prerequisites for access to classified or sensitive information).

## Analysis

### Guideline M—Use of Information Technology Systems

The security concern for use of information technology systems is set out in ¶ 39:

> Noncompliance with rules, procedures, guidelines or regulations pertaining to information technology systems may raise security concerns about an individual's reliability and trustworthiness, calling into question the willingness or ability to properly protect sensitive systems, networks, and information. Information Technology Systems include all related computer hardware, software, firmware, and data used for the communication, transmission, processing, manipulation, storage, or protection of information.

The government and his employer relied on him as systems administrator to comply with the policies and procedures concerning use of the information technology system. Applicant violated government policies as well as an agreement he signed in October 2002 concerning authorized use of a government-owned information resource asset when he improperly and repeatedly surfed the Internet for personal use during work hours in 2004. In addition to viewing news, sports, entertainment, and travel sites, he accessed over 500 sexually explicit prohibited web addresses using his government work computer between October 5, 2004, and December 23, 2004, if not before. He knew his use of the non-secure government computer was for business purposes only and he had agreed in writing to abide by this restriction. He also knew access to sexually explicit web sites was prohibited. AG ¶ 40(e) ("unauthorized use of a government or other information technology system") applies.

There is no evidence of any misuse of a work computer by Applicant since he started with his present employer in March 2005. While the passage of time is a mitigating condition (*see* AG ¶ 41(a) ("so much time has elapsed since the behavior happened, or it happened under unusual circumstances, such that it is unlikely to recur and does not cast doubt on the individual's reliability, trustworthiness, or good judgment")), his knowing disregard of policies prohibiting unauthorized use continues to cast doubt about his personal judgment. He has not shown any efforts to address the issues raised by his repeated access to prohibited adult sites at work. When interviewed in October 2006, he claimed pornography was not a big interest of his, but his access to

over 500 sexually explicit prohibited web addresses on his work computer suggests a problem Applicant is unwilling to acknowledge or deal with. He rationalized his behavior in his mind as long as the work was getting the work done. He has since apologized for his "terrible mistake," but missing from his apology ("The loss of my job, embarrassment to myself and family, and subsequent three month period of unemployment taught me a stern lesson." Item 4), is any meaningful appreciation for the extent to which he violated his fiduciary obligations. None of the mitigating conditions under AG ¶ 41 apply. His Internet surfing, to include of prohibited adult sites, cannot reasonably be characterized as minor and it was not done in the interest of organizational efficiency (*see* AG ¶ 41(b)). AG ¶ 41(c) applies only to unintentional or inadvertent conduct.

**Guideline E—Personal Conduct**

The security concern for personal conduct is set out in AG ¶ 15:

> Conduct involving questionable judgment, lack of candor, dishonesty, or unwillingness to comply with rules and regulations can raise questions about an individual's reliability, trustworthiness and ability to protect classified information. Of special interest is any failure to provide truthful and candid answers during the security clearance process or any other failure to cooperate with the security clearance process.

Applicant's knowing misuse of a government information resource system and computer for nine months to a year in 2004 also raises security significant personal conduct concerns of the type contemplated in AG ¶¶ 16(d)(3) ("a pattern of dishonesty or rule violations") and 16(d)(4) ("evidence of significant misuse of Government or other employer's time or resources"). Yet, since his misuse of the computer is explicitly covered under AG ¶ 39 of Guideline M, *supra*, it does not fall squarely within the concerns addressed in AG ¶ 16(d), which applies on its face to "credible adverse information that is not explicitly covered under any other guideline and may not be sufficient by itself for an adverse determination. . . ." The overall security concern under AG ¶ 15 is clearly implicated, however.

Personal conduct concerns may also be raised where there is evidence of "concealment of information about one's conduct, that creates a vulnerability to exploitation, manipulation, or duress, such as (1) engaging in activities which, if known, may affect the person's personal, professional, or community standing." (AG ¶ 16(e)). Unauthorized use of a computer involving access to pornography at work is information that clearly could negatively affect his standing with his family and colleagues. Applicant maintains he is not vulnerable to coercion, calling attention to the following language in the investigator's report (Item 6): "The investigation report of 11/1/06 stated 'He has learned his lesson. His wife and boss know about the details of the termination. This information could not be used for blackmail or coercion.'" When read in context, the investigator was not stating her own conclusions as to Applicant's potential vulnerability but rather merely reporting what Applicant told her. The available record, which includes the report of his interview, sheds no light on what Applicant told his spouse or his boss.

His uncorroborated generalization that his spouse and supervisor know of the details of his employment termination is insufficient to mitigate the vulnerability concerns under AG ¶ 17(e) ("the individual has taken positive steps to reduce or eliminate vulnerability to exploitation, manipulation, or duress").

Applicant's violations of the government's policies concerning authorized use of its information systems resources are not mitigated under AG ¶ 17(c) ("the offense is so minor, or so much time has passed, or the behavior is so infrequent, or it happened under such unique circumstances that it is unlikely to recur and does not cast doubt on the individual's reliability, trustworthiness, or good judgment"). Again, despite the passage of time, it continues to raise doubts about his reliability, trustworthiness, and judgment. His acknowledgment of the behavior satisfies only the first prong of AG ¶ 17(d) ("the individual has acknowledged the behavior and obtained counseling to change the behavior or taken other positive steps to alleviate the stressors, circumstances, or factors that caused untrustworthy, unreliable, or other inappropriate behavior, and such behavior is unlikely to recur"). He spent a considerable amount of work time in unsanctioned activity and has presented little to overcome the concerns.

**Whole Person Concept**

Under the whole person concept, the administrative judge must evaluate an applicant's eligibility for classified access by considering the totality of the applicant's conduct and all the circumstances. The administrative judge should consider the nine adjudicative process factors listed at AG ¶ 2(a):

> (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 extent to which participation is voluntary; (6) the presence or absence of rehabilitation and other permanent 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.

Under AG ¶ 2(c), the ultimate determination of whether to grant eligibility for access to classified information must be an overall commonsense judgment based upon careful consideration of the guidelines and the whole person concept.

I have evaluated Applicant's conduct under the whole person concept, applying the conclusions set forth previously in this analysis. Applicant indicates he learned a "stern lesson" from his mistake, and he acknowledged his unauthorized Internet access when he was interviewed by a government investigator and when he answered the SOR. Security clearance decisions are not intended to punish for past misconduct, but Applicant presented little to show that he can be counted on to abide by the ethical and fiduciary obligations of a security clearance.

## 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: | AGAINST APPLICANT |
| Subparagraph 1.a: | Against Applicant |
| Paragraph 2, Guideline E: | AGAINST APPLICANT |
| Subparagraph 2.a: | Against Applicant |

## Conclusion

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 Applicant eligibility for a security clearance. Eligibility for access to classified information is denied.

_____
ELIZABETH M. MATCHINSKI
Administrative Judge