DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 09-03136
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Daniel Crowley, Esq., Department Counsel
For Applicant: Alan V. Edmunds, Esq.

April 29, 2011

Decision

COACHER, Robert E., Administrative Judge:

Applicant failed to mitigate the security concerns under Guideline M, Use of Information Technology Systems and Guideline E, Personal Conduct. Applicant's eligibility for a security clearance is denied.

Statement of the Case

On August 6, 2010, the Defense Office of Hearings and Appeals (DOHA) issued Applicant a Statement of Reasons (SOR) detailing security concerns under Guideline M, Use of Information Technology Systems, and Guideline E, Personal Conduct. DOHA acted 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 adjudicative guidelines (AG), effective within the Department of Defense on September 1, 2006.

Applicant answered the SOR on August 20, 2010. He requested a hearing before an administrative judge. The case was assigned to me on January 18, 2011. DOHA issued a notice of hearing on January 20, 2011, with a hearing date of February 15, 2011. The hearing was convened as scheduled. The Government offered exhibits (GE) 1 through 3, which were admitted into evidence without any objection. Department Counsel's exhibit index was marked as hearing exhibit (HE) I. Applicant testified, presented one witness, and offered exhibits (AE) A through V that were admitted into evidence without any objections. Applicant's exhibit list was marked as HE II. DOHA received the hearing transcript (Tr.) on February 23, 2011.

Findings of Fact

In Applicant's answer to the SOR, he denied all the allegations, although he did admit specific facts in ¶¶ 1.a and 1.b. After a thorough and careful review of the pleadings, testimony, and exhibits, I make the following findings of fact.

Applicant is 55 years old. He has been married for 27 years. He has three adult children. He currently works for a defense contractor as a senior manager. He began working for his current employer in September 2008. Before that, he worked for a different defense contractor from 1979 to 2008 as the director of engineering. He was terminated from that position because he violated the company's policy related to improper Internet and computer use. The only severance he received from the company was accrued vacation pay. He did not pursue any grievance or other legal action against the company. He holds a bachelor's degree in chemical engineering. He has no military service. He has held a top security clearance since 2003.[1]

Applicant's conduct raised in the SOR includes: (1) viewing approximately 6,000 pornographic images while using a company computer in violation of company policy and installing an unauthorized software program on his company computer, also against company policy (SOR ¶¶ 1.a, 1.b, and 2.a); (2) making false statements on a security clearance application concerning the reason he was terminated from his employment in 2008 (SOR ¶ 2.b).

In February 2008, Applicant returned from a business trip. He carried a company laptop computer with him on the trip. The company had a written policy in place since March 2005 prohibiting the use of company computers to view pornography, a violation of which could result in immediate termination. On two separate occasions, Applicant indicated he was aware of this policy (when he was interviewed by an investigator for his security clearance in March 2009 and when he was confronted by management about the pornographic images found on his computer in February 2008); however, he testified that he was unaware of the policy until he was terminated in February 2008. I find his testimony on this point not credible.[2]

[1] Tr. at 37, 49; GE 1, 3.

[2] Tr. at 53-54; GE 2, 3.

When Applicant plugged his computer into the company's computer network, a virus was released from his computer to the network. The virus sent out mass emails throughout the network. The virus was traced to his computer and an investigation ensued by the company information technology team. On February 15, 2008, Applicant met with the company's human resource manager and was terminated for violating company policy by viewing pornographic images on his company computer and by putting unauthorized software on his company computer. He received a termination letter on February 15, 2008. The letter stated that over 4,000 pornographic images were found on his computer. Additionally, a search of a different hard drive associated with Applicant revealed 2,000 more pornographic images. The letter also explained that an unauthorized internet history cleaner software program was found on the computer. According to the letter, Applicant admitted to installing the program, viewing the pornography, and being aware that his actions violated company policy.[3]

Applicant's explanation for the presence of the pornography on his computer was because he received emails from a neighbor who would link to these pornographic sites. He claims his viewing was unintentional. He would check his personal email account when out of town on business using his company computer (this was allowed under the company policy). He would see emails from this neighbor and open them. Most of the time these emails were jokes or on some other neutral subject, but occasionally they contained links to prohibited sites. Even though Applicant knew that this neighbor would send an email that could contain links to prohibited sites, he continued to open those emails and view those links. He cannot really explain why he did that. Over a three year period he received about one email a month from this neighbor. He also claimed that the huge number of images found (6,000) resulted from the numerous thumbnail images that appeared on a page once the link was opened.[4]

Applicant installed the cleaner software program on his computer because he found that his computer was slowing down. He asked an information technician to look at his computer. According to Applicant, the technician suggested that he install the cleaner software program to clean up old web site and email clutter. The technician said that other company employees were using the software. Based upon this recommendation, Applicant downloaded the program onto his computer.[5]

Applicant sought new employment with a different defense contractor. In September 2008, he was required to fill out a security clearance questionnaire (SF-86). When asked whether he was ever fired from a job, he responded affirmatively that he was "Fired from a job." He further explained, "Used a non-classified company provided

[3] GE 3.

[4] Tr. at 39-40, 51, 57-58; GE 2, 3.

[5] Tr. at 44; GE 2.

laptop to view e-mail and do personal business (bill pay, etc) while on company travel." He denies intentionally trying to deceive the Government with those answers.[6]

Applicant called one witness who testified that he recommended Applicant for a security clearance. He worked with Applicant at his former company as the facilities security manager. He worked with Applicant when Applicant was terminated from employment. He has known Applicant for 15 years. He was aware of the company's policy prohibiting viewing pornography on company computers.[7]

In October 2010, in preparation for this hearing, Applicant received a psychological evaluation. The doctor's report concludes Applicant's behavior does not meet the criteria for any DSM-IV-TR diagnosis. It goes on to state, "His consumption of erotic imagery is mentionable not per se but because he used a company resource to consume it and because he knew his spouse would disapprove if she knew."[8]

Applicant presented the statements of several friends, neighbors, coworkers, and former coworkers. All the statements recommend him for a security clearance. He is characterized as loyal, trustworthy, and honest. Applicant also provided his performance appraisals from 2009 to 2011 that show an overall performance of "Meets Requirements."[9]

Policies

When evaluating an applicant's suitability for a security clearance, the administrative judge must consider the adjudicative guidelines. In addition to brief introductory explanations for each guideline, the adjudicative guidelines list potentially disqualifying conditions and mitigating conditions, which are used 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 commonsense 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.

[6] Tr. at 8; GE 1.

[7] Tr. at 21-35.

[8] Tr. at 49; AE B, C.

[9] AE D-N, Q-V.

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.

Under Directive ¶ E3.1.14, the Government must present evidence to establish controverted facts alleged in the SOR. Under Directive ¶ E3.1.15, an "applicant is responsible for presenting witnesses and other evidence to rebut, explain, extenuate, or mitigate facts admitted by applicant or proven by Department Counsel, and has the ultimate burden of persuasion to obtain 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 that an applicant may deliberately or inadvertently fail to 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

AG ¶ 39 expresses the security concern pertaining to use of information technology systems:

> Noncompliance with rules, procedures, guidelines or regulations pertaining to information technology systems may raise security concerns about an individual's reliably 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.

AG ¶ 40 describes conditions that could raise a security concern and may be disqualifying. I have especially considered the following:

(e) unauthorized use of a government or other information technology system; and

(f) introduction, removal, or duplication of hardware, firmware, software, or media to or from any information technology system without authorization, when prohibited by rules, procedures, guidelines or regulations.

Applicant used his company computer to view pornographic images. Applicant believed he was given permission by the information technician to install the cleaner software program. AG ¶ 40(e) applies, but AG ¶ 40(f) does not apply.

I have considered all of the mitigating conditions under AG ¶ 41 and especially considered the following:

(a) so much time has elapsed since the behavior happened, or it happened under such unusual circumstances, that it is unlikely to recur and does not cast doubt on the individual's reliability, trustworthiness, or good judgment; and

(c) the conduct was unintentional or inadvertent and was followed by a prompt, good-faith effort to correct the situation and by notification of supervisor.

Applicant's conduct was discovered in 2008. He viewed thousands of pornographic images on his company computer before that time. The events are recent enough, given the number, and there is insufficient evidence to convince me that the behavior will not recur. Applicant did not convince me that his behavior was unintentional, again, given the number of images viewed and his version of how he obtained the emails. Even if his actions were unintentional, there is no evidence showing his good-faith effort to correct the situation or efforts to notify a supervisor. AG ¶¶ 41(a) and 41(c) do not apply.

Guideline E, Personal Conduct

AG ¶ 15 expresses the security concern for personal conduct:

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.

AG ¶ 16 describes conditions that could raise a security concern and may be disqualifying in this case. The following disqualifying conditions are potentially applicable:

(a) deliberate omission, concealment, or falsification of relevant facts from any personnel security questionnaire; and

(e) personal conduct, or 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, or (2) while in another country, engaging in any activity that is illegal in that country or that is legal in that country but illegal in the United States and may serve as a basis for exploitation or pressure by the foreign security or intelligence service or other group.

Applicant's conduct of viewing pornographic material on a company computer created a vulnerability to his personal standing. AG ¶ 16(e) applies to SOR ¶ 2.a. Applicant's answers to the security clearance questions related to his firing were not false or misleading. He stated he was fired for violating company policy. He was not required to provide a more extensive explanation. The Government was put on notice of this incident. AG ¶ 16(a) does not apply.

The guideline also includes conditions that could mitigate security concerns arising from personal conduct. I have considered all of the mitigating conditions under AG ¶ 17 and especially considered the following:

(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;

(d) the individual has acknowledged the behavior and obtained counseling to change 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;

(e) the individual has taken positive steps to reduce or eliminate vulnerability to exploitation, manipulation, or duress; and

(f) the information was unsubstantiated or from a source of questionable reliability.

Applicant's viewing of 6,000 images on his company's computer in violation of company policy is not minor, given that he was terminated because of his actions. It is also recent enough to be of concern. The number of images on the computer led to the conclusion that this was not an infrequent activity for Applicant. AG ¶ 17(c) does not apply. Applicant did not really acknowledge his behavior, testifying that his viewing of the pornographic images was inadvertent and that he was unaware of the policy prohibiting pornography on company computers. Although he received a physiological

evaluation, there is no record evidence showing that he received counseling. AG ¶ 17(d) does not apply. Applicant informed his wife and friends about his actions, thus reducing his vulnerability to exploitation, manipulation, or duress. AG ¶ 17(e) applies. Applicant questioned the accuracy of the quantitative information contained in his termination letter concerning the number of pornographic images found on his computer. However, the letter was a business record used to terminate Applicant's employment. Applicant gave me no valid reason to view the information as unsubstantiated or unreliable. AG ¶ 17(f) does not apply.

Whole-Person Concept

Under the whole-person concept, the administrative judge must evaluate an applicant's eligibility for a security clearance 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 a security clearance must be an overall commonsense judgment based upon careful consideration of the guidelines and the whole-person concept.

I considered the potentially disqualifying and mitigating conditions in light of all the facts and circumstances surrounding this case. I considered Applicant's service to his company before the events that led to his termination. I also considered the seriousness of his actions resulting in the termination. Additionally, I considered his current performance evaluations and the strong recommendations he received from friends and coworkers concerning his honesty, reliability, and trustworthiness. However, Applicant's actions were violations of the clear company policy against viewing pornography on his company computer. Based upon the number of images found on his computer, I conclude he engaged in this activity on a regular basis. Applicant did not meet his burden to provide sufficient evidence to mitigate the security concerns.

Overall, the record evidence leaves me with questions and doubts about Applicant's eligibility and suitability for a security clearance. For all these reasons, I conclude Applicant did not mitigate the security concerns arising under Guideline M, Use of information Technology, and Guideline E, Personal Conduct.

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
Subparagraph 1.b:	For Applicant
Paragraph2, Guideline E:	AGAINST APPLICANT
Subparagraph 2.a:	Against Applicant
Subparagraph 2.b:	For 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.

_____
Robert E. Coacher
Administrative Judge