DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
----------	)	ISCR Case No. 08-11135
SSN: ----------	)	
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Braden M. Murphy, Esq., Department Counsel
For Applicant: Elizabeth L. Newman, Esq.

March 11, 2010

Decision

MARSHALL, Jr., Arthur E., Administrative Judge:

Applicant completed a questionnaire for sensitive positions (SF-86) on or about April 10, 2007. On March 17, 2009, the Defense Office of Hearings and Appeals (DOHA) issued a Statement of Reasons (SOR) enumerating security concerns arising under Guideline M (Use of Information Technology Systems) and Guideline E (Personal Conduct). 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 for SORs issued after September 1, 2006.

In his April 18, 2009, response to the SOR, Applicant substantially admitted the allegation set forth under Guideline M in SOR allegation ¶ 1.a and admitted SOR allegation ¶ 1.b in part. With regard to the allegations under Guideline E, Applicant wrote that he incorporated his responses to allegations ¶¶ 1.a-1.b with reference to allegation ¶ 2.a, and he substantially admitted the allegations set forth under ¶ 2.b. He also requested a hearing. DOHA assigned the case to me on September 9, 2009. The government moved for a delay in scheduling the hearing until its witness was available.

The request was granted without objection. The parties agreed to a hearing date of December 1, 2009. A notice of hearing to that effect was issued on November 9, 2009. The hearing was convened as scheduled.

Department Counsel introduced five documents accepted into the record without objection as exhibits (Exs.) 1-5. It also produced one witness. Applicant was represented by counsel, who offered two documents accepted into the record without objection as Exs. A-B. A witness provided testimony on behalf of Applicant. The parties were given through December 9, 2009, to submit any other documents, but none were offered. A transcript (Tr.) of the proceeding was received on December 10, 2009. The record was closed on December 14, 2009. Based on a review of the testimony, submissions, and exhibits, I find Applicant failed to meet his burden regarding the use of information technology systems and personal conduct security concerns raised. Security clearance is denied.

Preliminary Motions

Applicant presented a motion *in limine* "for an order (1) drawing an adverse inference in Applicant's favor, and (2) precluding Department Counsel from calling" his witness for the government. The basis for the motion was that Department Counsel intended "to elicit evidence from [the witness] as to the content of . . . [a] web site whose link he discovered on the lap top and/or hard drive that Applicant turned into him when Applicant resigned from his position. . . ." [1] The witness' testimony was opposed because the witness "engaged in spoliation by irrevocably erasing these items when he 'cleaned' the computer and hard drive, so that they no longer exist and cannot be introduced into evidence."[2] Applicant argued that it would violate his due process rights to allow the person who "destroyed evidence to testify, untrammeled, as to what he allegedly saw."[3]

Decision on the motion was deferred because the full scope of the witness' testimony was unknown. The parties were advised, however, that the witness' testimony would be permitted and given "appropriate weight" to the extent that it clarified the company's protocols for both cleaning and investigating the contents of company computers, and explained what he claimed he found on the computer.[4] In light of Applicant's admission he accessed pornographic web sites "to access pornography" on his employer's laptop computer at some point or points between 2006 and 2007, witness testimony was unnecessary to establish pornography was accessed by Applicant on his former employer's computer equipment. The witness' testimony on both direct and cross examination was ultimately accepted into the record only to confirm Applicant's admission regarding the types and forms of files accessed on the

[1] Motion, dated Nov. 25, 2009; Tr. 12-15.

[2] *Id,*

[3] *Id.*

[4] Tr. 16-18.

company's equipment and to elaborate on company protocols for reassigning previously assigned computer equipment.

At the hearing, Applicant moved that the SOR be amended to delete any reference to child pornography. Department Counsel stated, "I'm not sure it matters at this point but that's probably appropriate."[5] In declining to proceed with regard to the child pornography portion of the charge, the government stated that it did "not believe that there was any child pornography" found on the information technology system at issue.[6] The allegation regarding child pornography was stricken from the SOR.[7]

Findings of Fact

Applicant is a 30-year-old man working in the areas of business intelligence and data integration for a software company that is a government contractor. He has worked with computers since 1998, when he was a sophomore in college and performed software and web site development. After school, for about three years, he managed his own company which dealt mainly with different types of computer systems work, file recovery, web development, and other information technology-related areas. In that capacity, he was entrusted to work in customers' homes unattended. He later worked as a software sales manager. Applicant has a bachelor of science degree. He is single with no children.

In about June 2006, Applicant started working for his previous employer. He was issued a company-owned laptop in July or August 2006, which he used at both his office and his home.[8] Two or three weeks after starting work, he was also issued a handbook regarding the rules and regulations concerning his use of the laptop which he "kind of flipped through."[9] Before "flipping through" the handbook, he was "required to sign a form" that he "understood the policies" dictated by his employer, including the use of business equipment and internet use.[10] Applicant denies any specific knowledge "of the section having to do with what you could or couldn't access or download with your computer," but acknowledges that he had "some general knowledge of what you could or couldn't use that computer for."[11] He assumed there was a policy prohibiting

[5] Tr. 23.

[6] Tr. 21.

[7] Tr. 25. The government conceded that the allegation of child pornography "does no longer exist as one of the elements of the SOR."

[8] Tr. 79-80. Applicant later testified that he personally acquired an external hard drive for the laptop at issue in April or May 2006, for which he later received reimbursement. He stated that he did not register the hard drive with his employer. Tr. 88.

[9] Tr. 78, 118.

[10] *Id.*

[11] *Id.*

the downloading of internet pornography.[12] His "general knowledge" was that he could use the computer for "work-related purposes, discretionally for personal use such as e-mail or maybe buying something like a book on amazon.com."[13] Applicant was generally aware of policies used by companies regarding pornography access. He knew it was not "okay" to use the computer to access pornographic web sites.[14]

Between September or October of 2006 until about the end of 2007, Applicant used the laptop at issue to access pornographic web sites. He viewed the proscribed content at home, where he lived alone, on at least six occasions.[15] He estimates that he downloaded "about 12 movie files," each consisting of about 500 megabytes.[16] He would use the work equipment for such materials when he could not access the internet on his own personal home computer.[17] Of the movie files, some were downloaded from the internet, while one or more were copied from his home computer onto the company's external hard drive.[18]

After receiving his interim security clearance in about May 2007, but prior to October 2007, Applicant served his employer as the Assistant Facility Security Officer.[19] In October 2007, he was named the Facility Security Officer.[20] In preparation for this advancement, he took an online class "that was really kind of an orientation to the Industrial Security Program. It wasn't specific to the Facility Security Officer."[21] He also received instruction from his predecessor. He did not receive specific training regarding the prohibition against using company-owned and provided computer equipment for accessing pornography.

In about November 2007, while using his employer's equipment to surf the internet for satiric web sites, he clicked on a pop-up or advertisement that took him to a

---

[12] Tr. 119.

[13] Tr. 79.

[14] *Id.*

[15] Tr. 81, 116. Applicant testified that he used his employer's laptop to access pornography from home "about six times." *Contrast* "I don't know how many times adult pornographic websites were accessed over the 1.5 years (6/06-12/07) of my employment on the . . . computer from my home." Ex. 2 (Attachment to Interrogatories of Jan. 15, 2009) During that same interview, Applicant noted that after reviewing his former employer's policies, the applicable policy states that a "violation can lead to disciplinary action." *Id*. He does not clarify whether the referenced violation is regarding personal use or pornography.

[16] Tr. 81-82.

[17] Tr. 116-117.

[18] Tr. 119-120. No evidence was offered demonstrating Applicant's home computer's anti-virus protection.

[19] Tr. 99.

[20] *Id.*

[21] Tr. 100.

website he now "speculates" is or was a website which has a name that can be construed as racially divisive or offensive.[22] There, he saw material that could be deemed racially insensitive.[23]

In storing his cache of pornographic materials on his employer's equipment, Applicant maintained two separate sections on his external hard drive: one for work and one for "personal things."[24] He never stored classified information on the hard drive and did not receive a security clearance until September 2007.[25] Before resigning and leaving his former place of employment, Applicant "removed everything from the computer that [he] was not told to leave on there."[26] He specifically left files related to the security office and demonstrative images that were on the internal hard drive of the computer. As a result, "everything was returned in the state in which [Applicant] got it."[27] His cache of pornography was deleted from the external hard drive, as was material from the site which could be interpreted as racially insensitive.[28] By simply deleting the material without the aid of a special "un-erase" program or formal "wipe down," the material was not protected from recovery. He was not expecting the machine to be audited and was unaware of a policy under which hard drives were or might be examined.[29]

As Applicant prepared to leave the company in late December 2007, he met with his successor for about 90 minutes to review the demonstration images, give him passwords, and show him how the programs and laptop worked.[30] Applicant then left the equipment with his successor. He ultimately received a receipt for the transfer of equipment.[31] Applicant's last day of employment with this entity was December 28, 2007. Applicant's successor was tasked to "go through" the virtual server images that comprise a virtual computer, including scripts, programs, source code and applications

---

[22] Tr. 82-83, 125-126.

[23] Tr. 84-85. In Interrogatories dated January 15, 2009, at Ex. 3, Applicant denied all knowledge of the website at issue and its content.

[24] Tr. 89.

[25] *Id.*

[26] Tr. 91.

[27] Tr. 92.

[28] *Id.*, Tr. 94 ("When you handed it over it no longer had any of the pornographic material or the [potentially racially insensitive internet site's] material on it, is that right?" "Yes. I deleted everything off the computer." Tr. 94. He "just dumped everything in [his] personal files" without looking to see what was in them. Tr. 111).

[29] Tr. 93.

[30] Tr. 94, 96.

[31] Tr. 98-99; Ex. A (Exit Checklist).

"to see what went where."[32] As a business practice, it was part of wiping "the entire image and re-ghost [it] with a new image with updated drivers, updated service packs" before the equipment was reassigned.[33] In the process, pornography was found.[34] At the end of that process, the hard drive was scrubbed of all information, including evidence of inappropriate access.[35]

Applicant did not know that the proscribed materials had been uncovered until he was interviewed in August 2008 as part of the security clearance process. Prior to that time, he did not disclose or acknowledge his use of his former employer's equipment to access prohibited material.

In acknowledging his use of his former employer's equipment to access and view pornographic films and content, Applicant states that "I think looking back on it, it was a mistake. I should have been familiar with the policy, I should have followed the policy."[36] He never used company-owned equipment to access pornography in prior or subsequent jobs. In his present employment, the company has a policy regarding the personal use of its property for accessing the internet "very similar" to his former employer's policy: "One of the things that it specifies is you not view pornographic material."[37] From the time he was granted a security clearance in 2007 until the present, no other adverse incidents have been reported.[38] Applicant does not think his viewing of pornography makes him vulnerable to blackmail.[39] A close personal friend testified that he has never known Applicant to be racially insensitive in any matter.[40]

The company's handbook is 38 pages in length. Under the section entitled "*Necessary Rules*," one complete page is entitled and discusses "*Internet Usage*."[41] Internet connections are identified as being primarily for business purposes. Employees are "advised to use discretion when connecting to the internet for personal use" and unauthorized use is "strictly prohibited."[42] The first example of unauthorized use is

---

[32] Tr. 40-41.

[33] Tr. 41-42.

[34] Tr. 43-44.

[35] The lack of existent evidence is irrelevant to the extent Applicant admits he downloaded pornography.

[36] Tr. 107.

[37] Tr. 123.

[38] Tr. 109.

[39] Tr. 110.

[40] Tr. 128-133.

[41] Ex. 5 (Handbook) at 33.

[42] *Id.*

"[c]onnecting to, posting, or downloading pornographic material."[43] Further, it is noted that all files downloaded from the internet must be checked for possible computer viruses. Under a section entitled "*Inspection*," it is noted that desks, cabinets, and "storage devices" may be provided for the convenience of employees, but remain the sole property of [the company]" and can be inspected by any agent or representative of the company at any time.[44] Any questions regarding policies could be directed to designated individuals.[45]

Policies

When evaluating an applicant's suitability for a security clearance, an 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. These guidelines are not inflexible rules of law. 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. Under AG ¶ 2(c), this 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.

The government must present evidence to establish controverted facts alleged in the SOR. 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. . . ."[46] The burden of proof is something less than a preponderance of evidence.[47] The ultimate burden of persuasion is on the applicant.[48]

---

[43] *Id.*

[44] *Id.* at 35.

[45] *Id.* at 7.

[46] *See also* ISCR Case No. 94-1075 at 3-4 (App. Bd. Aug. 10, 1995).

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

[48] ISCR Case No. 93-1390 at 7-8 (App. Bd. Jan. 27, 1995).

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 an 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). "The clearly consistent standard indicates that security clearance determinations should err, if they must, on the side of denials."[49] Any reasonable doubt about whether an applicant should be allowed access to sensitive information must be resolved in favor of protecting such sensitive information.[50]

Based upon consideration of the evidence, Guideline F (Financial Considerations) is the most pertinent to this case. Conditions pertaining to this adjudicative guideline that could raise a security concern and may be disqualifying, as well as those which would mitigate such concerns, are set forth and discussed below.

Analysis

Guideline M – Use of Information Technology Systems

Under Guideline M, "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 *p*roperly protect sensitive systems, networks, and information."[51] It further notes that "Information Technology Systems include all related computer hardware, software, firmware, and data used for the communication, transmission, processing, manipulation, storage, or protection of information."[52] The Directive sets out several potentially disqualifying conditions under this guideline. Here, Applicant admits he accessed pornography on his former employer's computer equipment through the internet and copied from his home computer while generally aware that such access was prohibited or essentially proscribed under company policy. He then maintained such files on his employer's equipment until his departure from the company.

[49] *Id*.

[50] *Id*.

[51] AG ¶ 39.

[52] *Id.*

Therefore, both Use of Information Technology Systems (UITS) Disqualifying Condition (DC) AG ¶ 40(e) (unauthorized use of a government or other technology system) and AG ¶ 40(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) apply. With such conditions raised, the burden shifts to Applicant to overcome the case against him and mitigate security concerns.

Applicant admitted he accessed pornography from the internet through company-owned equipment. He similarly copied pornographic material onto his company's information systems from his personal computer. He denies having read the 38-page employee handbook, of which he acknowledged receipt, but admits that he assumed there was a prohibition against accessing pornographic material in this manner.[53] Moreover, the incidents at issue are multiple in number and occurred between the autumn of 2006 and the end of 2007. The repeated incidents were sufficiently recent and conducted with adequate notice of his company's policy to raise serious concerns regarding Applicant's judgment and ability to understand and appreciate established rules and policies. Such facts and concerns obviate application of UITS mitigating condition (MC) AG ¶ 41(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).

In accessing pornography from the internet, and in transferring pornographic at home, Applicant violated clearly enunciated policies regarding the improper and unauthorized use of the internet with company-owned equipment. Such policies were clearly set forth in the employee handbook, receipt of which he acknowledges. The contents of such a handbook are not optional considerations posed by the equipment's rightful owner or suggestions for professional conduct. They are rules to be read and followed. Moreover, Applicant's access of pornography carried with it the very real possibility of compromising the employer's information systems through viruses and other internet-bred problems. His access of such material was intentional and not in furtherance of his employer's mission. It was covertly acquired, deleted, and never reported. Consequently, neither AG ¶ 41(b) (the misuse was minor and done only in the interest of organizational efficiency and effectiveness, such as letting another person use one's password or computer when no other timely alternative was readily available) nor AG ¶ 41(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) apply.[54] Therefore, none of the mitigating conditions apply.

[53] Regardless, in neglecting to read the handbook, Applicant proceeded at his own peril.

[54] The only inadvertent activity suggested involves the potentially racially divisive web site that Applicant conceded he may have visited. Inasmuch as there is insufficient evidence that Applicant actually visited this site, however, that portion of the allegation is found in favor of Applicant.

Guideline E – Personal Conduct

Under Guideline E, "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."[55] Here, Applicant received and acknowledged an employee handbook he chose not to read. In violation of clearly detailed policy regarding the use of the internet with company-owned equipment, he accessed pornography on his employer's computer equipment from the internet and his home computer. Applicant failed to identify the dates of such access, but admits the conduct occurred between the autumn of 2006 and the end of 2007. That time frame suggests that some, if not all, of that material was accessed during this period or at least remained on his employer's equipment until he left his job. It is also significant because between about May 2007 and late December 2007, he served as his employer's Assistant Facility Security Officer, then as the Facility Security Officer. Although these facts are not amenable to the situations contemplated in the enumerated disqualifying conditions, such conduct raises the general security concerns noted in AG ¶ 15, above, regarding questionable judgment, lack of candor, and dishonesty or unwillingness to comply with rules and regulations that can raise questions about an individual's reliability, trustworthiness, and ability to protect classified information.

The same reasons set forth in the preceding section regarding UITS obviate applicability of Personal Conduct (PC) mitigating condition (MC) AG ¶ 17(c) (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). Moreover, while Applicant now freely admits his misconduct and stresses that his misuse of his employer's equipment to view pornography does not make him vulnerable to blackmail, it is notable that this disclosure and admission was not made until after his undisclosed deletion of the pornographic files and their ultimate discovery. At best, such after-the-fact efforts only raise AG ¶ 17(e) (the individual has taken positive steps to reduce or eliminate vulnerability to exploitation, manipulation, or duress) in part. None of the other mitigating conditions apply.

Whole Person Concept

Under the whole person concept, an administrative judge must evaluate an applicant's eligibility for a security clearance by considering the totality of an applicant's conduct and all the circumstances. An 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

[55] Revised Adjudicative Guideline (AG) ¶ 15.

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 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, as well as the "whole person" factors. Applicant is a well-educated man with significant professional experience in information technology and computers. At the time at issue, Applicant was in his late 20s and had worked in the information technology arena since he was a sophomore in college. He later managed his own business in that field. Applicant admits he accessed pornography with his employer's computer equipment. He also acknowledges that he signed a form stating he understood the contents of the employee handbook, but seeks to mitigate concerns by stating he never read the handbook before or after its initial receipt. Such facts, however, do not reduce concerns. They only highlight his unreliability and lack of appreciation for rules and policies. This is particularly true given Applicant's experience in the field, the fact he was generally aware that such activity was not authorized, and his personal assumption that there was a policy prohibiting the downloading of pornography.

Applicant did not simply access and maintain pornography as an idle employee by day or unthinking employee at night. He intentionally accessed and/or transferred pornography improperly in the privacy of his home, away from the workplace in which his activities might be observed. In deleting the material, he did so in a cursory manner. He did not think his employer would ever examine its own equipment. Application of professional common sense and a skim through the employee handbook, however, should have apprised him that his employer reserved the right to inspect its property at any time. Of particular concern is the fact that Applicant accessed pornography while serving as a trusted information technology professional and applicant for a security clearance who would eventually serve as the Assistant Facility Security Officer, then as the Facility Security Office. In those capacities, he violated company policy concerning internet usage, maintained pornographic material, failed to disclose its acquisition or maintenance, and ultimately tried to conceal its acquisition prior to his departure. In doing so, he demonstrated poor judgment, unreliability, and betrayed the trust of his employer.

The way in which the company discovered Applicant's misuse of its internet-capable equipment is relatively irrelevant. The employer had a right to inspect its own property. The fact that the evidence has since been scrubbed is similarly irrelevant. Applicant freely admitted to his conduct. While he has worked for another company for about two years without incident, insufficient time has passed to demonstrate that Applicant no longer misuses information technology systems, fully appreciates employer policies, and follows established company procedures. Given his background, profession, work responsibilities, and positions, Applicant's flagrant disregard of his employer's policies, his lack of concern regarding his equipment use, or his general

negligence raise and sustain genuine security concerns regarding both his use of information technology systems and his personal conduct. Therefore, it is concluded that security concerns raised by Applicant's access of pornography remain unmitigated. 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:	AGAINST APPLICANT
Subparagraph 1.a – 1.b	Against Applicant
Paragraph 2, Guideline E:	AGAINST APPLICANT
Subparagraph 2.a – 2.b	Against Applicant

Conclusion

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

ARTHUR E. MARSHALL, JR.
Administrative Judge