DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
----------	)	ISCR Case No. 07-03531
SSN: ----------	)	
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Eric H. Borgstrom, Esquire, Department Counsel
For Applicant: *Pro Se*

August 24, 2009

Decision

MATCHINSKI, Elizabeth M., Administrative Judge:

Applicant resigned from federal civilian employment in February 2005 following a history of inappropriate access of pornographic images using his government computer. He shows little remorse and has not been completely candid about his misconduct. Clearance is denied.

Statement of the Case

Applicant submitted his security clearance application (SF 86) on January 23, 2003. On December 17, 2008, the Defense Office of Hearings and Appeals (DOHA) issued to Applicant a statement of reasons (SOR) detailing the security concerns under Guideline M that provided the basis for its preliminary decision to deny him a security clearance and refer the matter to an administrative judge. 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 as of September 1, 2006.

Applicant submitted an undated response to the SOR that was received by DOHA on February 18, 2009. He requested a hearing, and on April 2, 2009, the case was assigned to me to determine whether it is clearly consistent with the national interest to grant or continue a security clearance for Applicant. On May 8, 2009, I scheduled a hearing for May 29, 2009.

I convened the hearing on May 29, 2009. Before the introduction of any evidence, the SOR was amended at the request of the government with no objection, *see infra*. The government submitted four exhibits (Ex. 1-4), Exhibits 1-3 were admitted without any objections. Applicant questioned the relevance of some information in Exhibit 4. Those statements within Exhibit 4 were stricken with the agreement of Department Counsel and the document was admitted. Applicant also testified, as reflected in a transcript (Tr.) received on June 8, 2009. For the reasons discussed below, eligibility for access to classified information is denied.

Procedural and Evidentiary Rulings

At the hearing, the government moved to amend the SOR to add a new paragraph 2 alleging a security concern under Guideline E:

> You falsified material facts during a February 1, 2007, interview with an investigator from the U.S. Office of Personnel Management when you denied having ever viewed pornography on the Internet.

On March 30, 2009, Applicant was furnished a copy of the motion in writing with those documents the government intended to offer into evidence at his upcoming hearing. Applicant did not object to the amendment. The motion was granted, and Applicant denied the allegation.

Findings of Fact

In the SOR as amended, DOHA alleged under Guideline M, use of information technology systems, that Applicant's employer seized his government computer in or about January 2005 to conduct a forensic investigation for unauthorized or inappropriate material (SOR ¶ 1.a); that the investigation revealed that he had accessed pornographic websites on the Internet (SOR ¶ 1.b); that he had used his government computer to access pornographic websites after he had completed mandatory computer training in November 2004 and been warned that such use was unauthorized (SOR ¶ 1.c); and that he had been verbally counseled in about 2002 for unauthorized use of his government computer (SOR ¶ 1.d). Under Guideline E, Applicant was alleged to have falsely denied during his February 1, 2007, subject interview that he had ever viewed pornography on the Internet (SOR ¶ 2.a). Applicant admitted the Guideline M allegations with explanations. Applicant was given an opportunity to respond to the

Guideline E allegation before the introduction of any evidence. He denied any intentional falsification. After consideration of the pleadings, exhibits, and transcript, I make the following findings of fact:

Applicant is a 37-year-old integration and test engineer who has worked for his current employer, a defense contractor, since mid-2005 (Tr. 40). He seeks to retain a top secret security clearance that was transferred to his work for his current employer (Tr. 94, 115).

Applicant earned his bachelor of science degree in electrical engineering in May 1994 (Exs. 1, 2). In August 1994, he began working as a civilian project engineer for the federal government (Ex. 1, Tr. 37-39). He was granted a secret-level security clearance for his duties in November 1994 (Ex. 2), and it was eventually upgraded to top secret (Tr. 115). On December 18, 1997, he applied for access to sensitive compartmented information (SCI) for his work with sensitive military programs (Ex. 2), and that access was granted in March 1998 (Ex. 1, Tr. 40-41).

In 2002, Applicant was verbally counseled by his supervisor for viewing inappropriate material on his work computer. Applicant cannot now recall whether the computer was provided by the government or by a contractor for the government. The connection was provided by the government (Tr. 44). When asked at his hearing whether he was viewing pornography on the Internet, Applicant responded, "It's entirely possible." (Tr. 44). Concerning whether he searched for images or opened electronic mail messages, Applicant indicated that "everyone had come in contact with adult oriented material at some time." (Tr. 47). Applicant testified that there were no specific policies about Internet use at that time ("things were pretty loose"), although they were not allowed to hack into a machine or download illegal material (Tr. 45). Applicant denies he downloaded inappropriate material onto his work computer at that time, or that he accessed child pornography (Tr. 49). No evidence was presented to the contrary.

In or before 2004, Applicant switched from a desktop to a laptop computer at work because of frequent travel. He kept the laptop at the office connected to a docking station when he was not on travel (Tr. 54). While on temporary duty overseas for his employer in the summer of 2004, Applicant downloaded a large batch of computer files from an external hard drive onto his government-provided laptop computer. The files, which had generic names or titles (Tr. 62), contained not only Hollywood movies but also home videos containing adult content. Applicant obtained the hard drive from a sailor at work and he was unaware of specific contents when he loaded it onto his work computer (Tr. 60-62). As Applicant went through the files, he noticed that some of them were adult oriented in nature (Tr. 58, 61), and he deleted them by dragging them into the trash folder and emptying the folder (Ex. 3, Tr. 58).[1] Applicant testified that he informed information technology employees on his return from temporary duty that he

[1]Applicant admitted that by deleting a file in that manner, it might still be on the computer's hard drive but that it would eventually be overwritten (Tr. 66).

had deleted the material and that he had exercised "due diligence in the circumstance" (Tr. 58).

In November 2004, Applicant completed annual mandatory computer security training that warned against unauthorized use of government computer systems (Ex. 4). In about late December 2004, Applicant's work laptop computer was seized by security personnel for a forensic investigation of possible inappropriate access. Applicant was given a new computer and allowed to continue working. Over the next few weeks, Applicant had been informed by his supervisor that inappropriate material had been found on his work computer (Ex. 3). The investigation of the seized laptop revealed that Applicant had been accessing pornographic websites via the Internet on his work laptop computer (Ex. 4).[2] At his May 29, 2009, hearing, Applicant would neither confirm nor deny whether he had accessed Internet websites containing pornography in late 2004:

> I may have, I may not have. One of the habits I had was in when I left my computer at work, was often my web browser was often not password protected, so I left my computer unattended. So I may have looked at something I shouldn't have or someone may have gotten into my computer at my expense (Tr. 53-54).

Applicant worked in a non secured area, although the building in which his cubicle was located had "swipe access" (Tr. 55). Applicant testified unrebutted by the government that his computer stayed logged on even when he was away from his desk (Tr. 56), but no evidence was presented to confirm that someone else accessed pornography using the laptop assigned to him.

In January 2005, the military command issued a security access eligibility report (SAER) to the service's adjudication component recommending that Applicant be found ineligible for continued SCI access because of his inappropriate access of pornographic web sites using his government computer. On February 2, 2005, Applicant resigned from his government position and his former employer forwarded the SAER to the service's adjudication component (Ex. 4). Applicant was aware at the time that inappropriate adult material had been found on his laptop (Ex. 3, Tr. 65),[3] but there is no evidence that he knew the SAER had been submitted.

---

[2]The report of the forensics investigation was not submitted into evidence. In an issue summary of August 23, 2005, a military adjudicator referred to the security access eligibility report (SAER) from Applicant's then employer which indicated that Applicant had been surfing the Internet accessing pornographic web sites and that he had been verbally counseled for the same problem about three years earlier (Ex. 4). The SAER was also not available for my review, but there is no apparent reason to doubt the accuracy of the adjudicator's summary of the SAER.

[3]Applicant initially claimed that he knew nothing at that time other than that the investigation was ongoing (Tr. 65), but he later acknowledged that his supervisor had told him that inappropriate adult material had been found on his laptop's hard drive (Ex. 3, Tr. 66). He later stated that the unauthorized access concerned one specific day when he was on annual leave (Tr. 90).

Applicant worked for a company for only a couple of months before going to work for his present employer in mid-2005. On February 1, 2007, Applicant was interviewed by a government investigator about his possible misuse of a government computer system. Applicant explained that he had downloaded files onto his work computer while on temporary duty overseas in the summer of 2004 that he thought contained "regular first-run movies" but he discovered included home videos with adult content. Applicant acknowledged that his laptop had been seized by security officials when he was at work "in late December 2005" [sic] and that over the next several weeks, he learned from his supervisor that security had found inappropriate adult material on the hard drive. He indicated that he resigned his federal employment voluntarily and not under any threat of discipline or termination. Applicant averred that he had told his supervisors at his subsequent employment (which he held for only a couple months, Tr. 38) about the incident. He denied ever introducing any unauthorized hardware, software or media into any information system, or that he had ever viewed pornography online (Ex. 3).

Applicant denies accessing pornography on the Internet at work since "sometime before 2005" (Tr. 69, 81). Applicant claims to have no recall of any direct instance of using a government computer to access a pornographic website after 2002 ("I mean I was, you know, after I had been counseled by that, I was pretty much scared straight." Tr. 81-82). He accessed pornographic websites at home within a week or two of his hearing in May 2009 (Tr. 69).

Applicant earned his master's degree in systems engineering in May 2009 (Tr. 36) while continuing to work for his present employer.

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 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.

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 about the 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.

Applicant improperly accessed pornography at work in 2002, for which he was counseled by his supervisor. Although not alleged as a security concern, Applicant downloaded a large batch of files, some containing adult images, onto his government laptop computer in the summer of 2004. His assertion that he was unaware of the adult content is difficult to accept, given his past history of viewing inappropriate adult material at work. Then in about early January 2005, he was found to have improperly

accessed pornography via the Internet on his work laptop computer. He testified that his employer might have found "some remnants of stuff that [he] had deleted a long time ago" (Tr. 66); that he might have had some "risque material" on there, which "if [he] were to really speculate, there may have been a picture or two of a girl in a bikini on a car" (Tr. 68). But neither circumstance gets to the root of his misconduct, which was inappropriate website access, possibly discovered initially through monitoring, whether routine or targeted, of Internet connectivity. Even assuming that Applicant left his computer logged on when unattended (Tr. 85), there is no evidence to substantiate his assertion that someone else may have used his computer to gain unauthorized access to pornography at work. 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 mid-2005. Yet, I am unable to fully apply 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." Applicant testified that after he was counseled about using a government computer to access a pornographic website in 2002, he was "pretty much scared straight." (Tr. 81-82). But the results of the forensic investigation of his work computer in late 2004 show this was not the case. Considerable judgment concerns persist because of his unwillingness to accept responsibility for his misuse of the government computer. Concerning his access to pornography through his work computer in and before 2002, Applicant blamed the lack of specific prohibitions ("I may have but then again, there were certainly times in my history, employment history, where that wasn't necessarily against the rules because there weren't any." Tr. 48). When asked whether he accessed pornography at work in 2004, Applicant responded, "I may have, I may not have." (Tr. 53). Applicant may not now be able to recall each instance, but he certainly knew whether or not he had accessed adult material on his work computer. His credibility is undermined by such equivocation, and by his suggestion that if he accessed pornography, it was unintentional:

> I clearly know the difference between a classified system and an unclassified system, the data access and work-related activities, the two have never mingled. This was an unclassified system, an unclassified network with no real firewall protection whatsoever, so there were, may have been, I should say, instances where adult oriented material may have been viewed unintentionally. I'm not really going to say that in my activities but certainly it's certainly possible (Tr. 86).

Applicant had been counseled in the past about viewing adult oriented content on his work computer, and he had recently completed training that advised against inappropriate use of the work computer. Applicant knew or should have known to use his government computer for official purposes, and his claim of inadvertent access is not persuasive. 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," does not apply.

Guideline E—Personal Conduct

The security concern related to the guideline 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.

When Applicant was interviewed on February 1, 2007, about possible misuse of a government computer system, he told the government investigator that he had downloaded batch files while on temporary duty in the summer of 2004 that unbeknownst to him contained files with adult images. As for the subsequent seizure of his computer, Applicant explained that he learned from his supervisor that inappropriate material had been found on his hard drive. After he explained what had happened while he was on temporary duty that summer, he heard nothing more about it and was not disciplined. He denied any intentional violation of any procedures regarding the use of computer systems, any introduction of unauthorized hardware, software, or media, into any information technology systems, or that he ever viewed pornography online. His denial of ever having viewed adult-oriented material via the Internet was false, and formed the basis for the government's recent amendment to the SOR. Applicant maintains that he understood the context of the question to be limited to whether he had viewed adult material at his present place of employment:

> The investigator did not ask me any questions regarding my Internet access at [government employer] and there are two reasons for that, either a: [government employer] had said so and he felt that that [sic] was not pertinent to his investigation or [government employer] themselves did not say so and did not inform the investigator and he didn't talk about that. So as we got later on in the interview and the investigation, we talked more about present tense circumstances, so I thought the question was in relation to my current employment with [company X], which had been several years in.(Tr. 75).

As discussed under Guideline M, *supra*, there is no evidence that Applicant ever accessed pornography at work since he started his present job in mid-2005. But while the investigator's report does not contain the specific questions asked of Applicant, it includes unequivocal denials by Applicant concerning whether he had ever given anyone unauthorized access, ever introduced any unauthorized hardware, software, or media into any information technology system, or ever viewed pornography online.

Applicant confirmed the accuracy of the investigator's report of his interview, and in that report it states, "HE HAS NEVER VIEWED PORNOGRAPHY ONLINE." No one reading the report of the interview would have any reason to know that Applicant's misuse of a government computer involved other than the inadvertent downloading of adult material while he was on temporary duty in 2004. His claim that it was a good faith mistake related to the scope of the inquiry is implausible, particularly in light of the fact that he had been counseled for inappropriate access in 2002. A finding of intentional concealment is reasonable based on the investigator's report, Applicant's suspect credibility regarding the issue of access to Internet pornography, and his confirmation of the accuracy of the investigator's report in August 2007. AG ¶ 16(a), "deliberate omission, concealment, or falsification of relevant 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," applies.

Applicant's misuse of a government information system raises judgment and reliability concerns (*see* AG ¶ 15) and is a "significant misuse of Government or other employer's time or resources" (see AG ¶ 16(d)(4), "credible adverse information that is not explicitly covered under any other guideline and may not be sufficient by itself for an adverse determination, but which, when combined with all available information supports a whole-person assessment of questionable judgment, untrustworthiness, unreliability, lack of candor, unwillingness to comply with rules and regulations, or other characteristics indicating that the person may not properly safeguard protected information. This includes but is not limited to consideration of: (4) evidence of significant misuse of Government or other employer's time or resources."). However, it was not alleged under Guideline E, and AG ¶ 16(d)(4) would not apply since the misuse of a government computer system is explicitly covered under ¶ 39, *infra*.

Applicant's failure to be up-front about his knowing misuse of the government-owned information system is not mitigated under AG ¶ 17(a), which requires that the effort at rectification be prompt, in good faith, and before confrontation ("the individual made prompt, good-faith efforts to correct the omission, concealment, or falsification before being confronted with the facts"). Applicant's employer, then the federal government, did not learn of Applicant's inappropriate web access from him. Applicant had the opportunity to candidly address this during his interview and instead denied he had ever accessed pornography online. At his hearing in late May 2009, he testified equivocally about whether he had viewed inappropriate adult material on his government computer. Even though more than four years have passed since Applicant's unauthorized use of a government information technology system, his violation of his fiduciary obligation of complete candor is recent and serious. 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," is not pertinent. At this point, the government is not yet fully aware of the circumstances or extent of his misuse of the government information system. He has shown little to no

appreciation for the seriousness of his trust violations, so 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," also does not apply.

Whole-Person Concept

Under the whole-person concept, the administrative judge must evaluate Applicant's eligibility for a security clearance by considering the totality of his conduct and all the circumstances in light of 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.

Applicant has raised considerable concerns about his judgment, reliability, and trustworthiness through his misuse of a government information technology system from at least 2002 to late 2004, and by dodging the obligation of full candor required of him by virtue of his top secret clearance. He has shown some corrective action in that he has not used a computer to access a pornographic website at work in more than four years, but it is not enough to fully mitigate the security concerns. Applicant has not always been the "good steward" (Tr. 86) of the government's trust. He has yet to understand the security implications of, and take responsibility for, his repeated misuse of a government information technology system.

Formal Findings

Formal findings for or against Applicant on the allegations set forth in the amended 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:	Against Applicant[4]
Subparagraph 1.c:	Against Applicant
Subparagraph 1.d:	Against Applicant
Paragraph 2, Guideline E:	AGAINST APPLICANT
Subparagraph 2.a:	Against Applicant

Conclusion

In light of 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

[4]SOR ¶¶ 1.a and 1.b pertain to the same conduct. The results of the investigation are reported in SOR ¶ 1.b and do not represent conduct of additional security concern.