DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
----------	)	ISCR Case No. 06-09685
SSN: ----------	)	
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Alison O'Connell, Esquire, Department Counsel
For Applicant: *Pro Se*

April 10, 2008

Decision

MATCHINSKI, Elizabeth M., Administrative Judge:

Applicant submitted his security clearance application (e-QIP) on November 21, 2005. On September 17, 2007, the Defense Office of Hearings and Appeals (DOHA) issued to Applicant a Statement of Reasons (SOR) detailing the security concerns under Guidelines E and M. 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 responded to the SOR in writing on October 11, 2007, and requested a decision based on the record without a hearing. On October 29, 2007, previously assigned Department Counsel requested a hearing. The government was prepared to proceed on December 7, 2007, and the case was assigned to me on December 20, 2007. On January 17, 2008, I scheduled a hearing for February 28, 2008.

The hearing was convened as scheduled. Two government exhibits (Ex. 1-2) and two Applicant exhibits (Ex. A-B) were admitted without any objections and Applicant testified, as reflected in a transcript (Tr.) received on March 10, 2008. At Applicant's request, the record was held open until March 13, 2008, for him to submit work performance evaluations and awards. On March 11, 2008, Applicant timely forwarded five documents. The government did not object to their admission, and they were received as Exhibits C through G. For the reasons discussed below, eligibility for access to classified information is denied.

Findings of Fact

DOHA alleged under Guideline E, personal conduct, that Applicant misused a government computer and system in April 2005 by posting sexually explicit material onto a server at work from a personal portable drive (SOR ¶ 1.a); that he misused the government computer by maintaining sexually explicit material on his government-owned work computer in April 2005 (SOR ¶ 1.b); that during an investigation into the posting of inappropriate adult material on the server he initially denied any involvement (SOR ¶ 1.c) and that he had saved the adult material on his work computer (SOR ¶ 1.d); and that he was terminated from his job because of his violations of company policies on the use of government equipment and his attempts to conceal facts during the company's investigation (SOR ¶ 1.e). The misuse of the government computer system by posting sexually explicit material on the server and by maintaining sexually explicit materials on his work station were also alleged under Guideline M, use of information technology systems (SOR ¶ 2.a).

Applicant provided a detailed answer indicating that he had inadvertently posted the sexually explicit material on his work computer. Working long hours at home, Applicant indicated he had transported non-sensitive files using his personal memory disks and that he unintentionally grabbed the folder containing sexually explicit material along with his work folder and copied both onto the portable media. While loading the work files onto the system, he also grabbed the folder with the sexually explicit material. As for maintaining sexually explicit material on his work computer, Applicant explained that the loading of files was accidental. Applicant admitted that during the company's investigation, he had initially denied he had loaded any adult material on the server, although after seeing the files he knew they were his but "still had no idea how they got there." Applicant admitted that inappropriate files had apparently been on his hard drive since he used his computer as an intermediary in moving from the media to the server, but he denied any awareness prior to the investigation. Applicant acknowledged his employment termination for a mistake that cost him and his family dearly. He indicated he was now "overly conservative" and never commingles files nor uses portable media. After consideration of the evidence of record, I make the following findings of fact:

Applicant is a 51-year-old senior systems engineer who has worked for his current employer, a defense contractor, since October 2005 (Ex. 1). He seeks a secret-level clearance for his duties in systems architecture and design, involving a military destroyer program (Tr. 19, 38, 43-44).

In May 1980, Applicant was awarded his bachelor of science degree in general engineering from a U.S. military academy (Ex. 1, Tr. 41-42). The following month, he married his first wife (Ex. 1). He served on active duty with a secret-level security clearance until May 1985 when he was discharged at the rank of captain (Ex. 1, Tr. 42).

In about 1992, Applicant went to work at a national laboratory for a company hired to oversee the contractors maintaining and operating the site for the U.S. government. Applicant stayed on at the facility under the employ of a succession of contractors that maintained the facility over the years. (Ex. 1, Tr. 44-45).

In June 1997, Applicant and his first wife divorced (Ex. 1). She had left him with their three children to raise on his own. His son was born in August 1988 and his two daughters were born in September 1990 and November 1993 (Ex. 1, Tr. 32, 42-43). In August 1997, Applicant married his second wife, but they divorced in September 2002. In July 2004, Applicant wed his current spouse, and his household expanded to include her four biological children. In December 2004, Applicant legally adopted her youngest, a boy born in November 1998 (Ex. 1, Tr. 43).

Applicant was happy in his new marriage, which included some sexual experimentation, taking pictures of themselves performing sexual acts, watching X-rated movies, and viewing sexually explicit material on their computer together (Tr. 32, 61, 71-72). So that his children were not exposed to this pornographic material, Applicant kept the sexually explicit images on personal portable media (a computer jazz drive) (Tr. 28-30, 51, 71). He testified most of the files were given a generic identifier, “like AA, A1" (Tr. 54). Applicant promised his spouse that he would not view any pornographic material by himself, but he intermittently viewed sexual images from his jazz drive on his desktop at work (Tr. 58-59). Applicant denies ever viewing pornographic websites at work (Tr. 58). He was unaware at that time that files accessed by the computer were cached (Tr. 28), but he knew it was against company policy to view pornographic material on his work computer (Tr. 60).

The information resources used by employees of the cleanup project were government property. Information resources included all government-owned or government-funded data communication equipment and services, located on or off site, including but not limited to personal computers, laptop computers, workstations, networking services, mainframes, associated peripherals and software, and government provided access to electronic mail, the intranet, and the Internet. Under section 1 of the employee handbook applicable to those on the cleanup project, government or company equipment was to be used for official business only. Employees were specifically advised in the handbook that the use of government equipment or services to intentionally access, download, or otherwise transmit any sexually explicit material would not be tolerated and would result in discipline up to and including discharge (Ex. 2).

As of April 2005, Applicant was involved in the clean up project at the laboratory where he oversaw and supported the lead on the chemical management system. With a

new contractor taking over in May 2005, Applicant had been looking at various commercial systems to manage and report the laboratory's hazardous and radiological waste, as the home-grown system had become very expensive to maintain (Tr. 47). Applicant put in long hours at work and home evaluating a commercial software system and the laboratory's requirements (Tr. 70). Applicant transported the information to work on at home via his personal jazz drive that also contained sexually explicit images. He kept the information segregated in different folders (Tr. 50).

On April 20, 2005, Applicant inadvertently posted a folder containing about 50 images and videos of a sexually explicit nature, including images ("four or five, or a dozen") of him and his spouse performing sex acts, onto the server at work (Tr. 60-61). While uploading onto the server the data he had worked on at home the night before, Applicant grabbed from his jazz drive not only the folder containing the work data, but also a folder on which he had stored sexual images and videos ("if you touch another folder that you didn't mean to, and if you don't notice that you did and you just grab and drag and drop it. . . .") (Ex. 2, Tr. 30-31, 50-51).[1] On April 26, 2006, another employee on the cleanup project found the inappropriate adult material on the laboratory's server,[2] and reported it. During an investigation, Applicant was linked with ownership of the folder through his user id and records showing that his office computer was logged onto the server when the folder was uploaded. Firewall logs for Applicant's work computer for 2005 to date did not show any access to obvious adult sites (Ex. 2).

Applicant was interviewed by the investigator on April 28, 2005. He was told up-front that the investigation concerned the posting of inappropriate adult material to a lab server and that if he was involved in that activity, he should tell him so. Applicant denied any involvement or any knowledge of it. After he was shown the titles of the material posted to the server, Applicant acknowledged that it was material from his home personal computer ("He showed them to me and I said I couldn't have done that, I keep them you know, I keep them all separate, and maybe, I had never saved them on my hard drive at work or anything else, so I was just in total shock. . . ." Tr. 53). Applicant surmised he brought it in by mistake with material he had taken home to work on, and denied he had purposely posted the files to the server. The investigator expressed his belief that Applicant had meant to save the sexual material on his work computer. Applicant responded that he would not save it to his personal computer as he did not view that type of material at work ("I don't know if it's more disbelief or I can't really tell you the emotional state at that point, but, no, I was not forthright at the interview. . . ." Tr. 73). After Applicant provided a written statement,[3] the investigator checked Applicant's work computer in his presence. The investigator found 129 adult images in a temporary folder that had been created on April 20, 2005, about 15 minutes before the

[1]Applicant testified that the material went straight from the portable drive onto the server and that nothing from the portable drive should have remained on his desktop's hard drive (Tr. 52).

[2]The inappropriate material did not include any child pornography (Ex. 2).

[3]This statement was not included in the evidentiary record available for review.

sexually explicit images appeared on the server. Twenty-eight MPEG files were found in a recent folder. The investigator determined the MPEG files had been viewed on the computer using Windows Media Player but were not presently on the computer. The titles of the files in the two folders on Applicant's work computer were then compared to the titles in the folder loaded on the server. Only two of the 129 JPEG files matched the names of JPEG images on the server, but one was not the same image and the other couldn't be viewed. There were some title matches in the other folder. Applicant was involuntarily terminated from his employment on May 9, 2005, for misuse of a government computer and system and attempt to conceal facts during the company's investigation, in violation of company policies (Ex. 2, Tr. 61).

Applicant was unemployed for a few months as he was unable to find another job in a close-knit town in which there were few opportunities outside of farming or the services industry that supported the national laboratory site. In October 2005, he began working for his present employer. Applicant regrets that he had to move his children across the country away from the only home and the friends they had known (Tr. 33, 63).

On November 21, 2005, Applicant completed an e-QIP in application for a secret-level security clearance. Applicant disclosed his termination from his previous employment in May 2005, for copying what he thought were work-related files onto the server but "[o]n that disk was some files of a personnal [sic] nature, including files that were pornographic." He explained that he did not realize what he had done until he was interviewed by an investigator, and that during the interview he was not as open as he should have been, mainly because of the embarrassment to him and his spouse. Applicant that he and his spouse no longer take any pictures of themselves, and regrets not being as forthright as he should have been (Ex. 1).

All but the youngest of Applicant's children are aware of the reason for his firing, although they don't know all the details (Tr. 34). Applicant has not told his present employer that he had been terminated from his previous job, although he maintains he would divulge it if he had to (Tr. 64). During the hiring process, he told his employer he needed a new job ("if you are seeking employment, you don't say, of, and by the way, you know, so no, unless you don't want the job") (Tr. 65).

Applicant no longer uses any portable media. His computer is located in a public area of the house (Tr. 34, 65). He also made an effort to educate himself about business ethics and computer systems in general (Tr. 34, 68). He has read his current employer's policies concerning information security, including business ethics, acceptable uses of the Internet, authorized limited personal use of company assets, corporate security, and control of company sensitive information (Ex. A). He also completed training offered by his employer, including introductory business ethics on December 15, 2005, code of conduct on September 28, 2006, ethical awareness and decision making on March 29, 2007, and information security awareness on May 31, 2007 (Ex. B).

Applicant's work performance over the past two years has been recognized by his employer (Ex. C, Ex. D, Ex. E, Ex. F, Ex. G). Once in 2006 and twice in 2007, he was given individual performer achievement awards for outstanding efforts on the proposals involving the military destroyer program (Ex. C, Ex. D, Ex. G).

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 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.

Applicant exercised extremely poor judgment by viewing pornographic images on a government-owned computer at work intermittently in 2005 (SOR ¶ 1.b). Unaware that the images were cached in the computer's memory, Applicant yet knew it was a misuse of a government information resource and against company policy to view sexually explicit images on his work computer.

In April 2005, he also uploaded sexually explicit images from his personal jazz drive onto a server at work (SOR ¶ 1.a). This was also a misuse of a government information system. It is not clear whether he was authorized to process work using his personal jazz drive.[4] Under section 1 of the employee handbook, bringing or using unauthorized personal computer hardware and/or software to work could subject an employee to suspension (*see* Ex. 2), but his use of a jazz drive containing sexually inappropriate material in a government system was clearly against company policy. During the government investigation, 129 adult images were found in a temporary file on Applicant's workstation computer. However, Applicant credibly testified he did not knowingly post the sexual images onto the server:

> He had asked did you put pornographic files on the server and I was like no, I didn't. I mean something like that, intentionally doing, you know, no, I just, no, I would never do that, that would be, you know, first of all, that would be stupid because I would know that, pardon the expression, it wouldn't be very smart because I know other people have access, that's our server that our team uses every single day to push information back

[4]Applicant indicated on his e-QIP that his supervisor was well aware that he was taking work home (Ex. 1), but this does not mean that his supervisor knew he was using a portable jazz drive that also contained pornographic images.

and forth, so it would be immediately visible to anybody and everyone within that group (Tr. 73).

Some of the sexually explicit images were of Applicant and his spouse, and he is unlikely to have knowingly transferred images that could possibly be recognized by a coworker. Since he did not realize that he had loaded the inappropriate adult images on the server until he was shown the titles of the material posted to the server, I find Applicant also did not intentionally fail to disclose to the investigator that the material was from his personal portable drive and that he had posted it onto the server. Yet, Applicant lied when he then indicated to the investigator that he had not viewed pornography on his work computer. Disqualifying condition AG ¶ 16(b) ("deliberately providing false or misleading information concerning relevant facts to an employer, investigator, security official, competent medical authority, or other official government representative") applies because of that falsification.

Applicant's use of his work computer to view pornography led to inappropriate adult images being maintained on the computer. His repeated rule violations involved significant misuse of government resources. Although this conduct raises judgment concerns of the type contemplated under 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"), ¶ 16(d) does not apply since the misuse of a government information system is explicitly covered under ¶ 39, *infra*.

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)). Applicant maintains, with no evidence to the contrary, that his spouse and all but the youngest of his children are aware to some degree of the circumstances leading to his termination from his previous employer. However, he has not volunteered to his current employer that he was fired from his previous position. While it is understandable that he would not want to divulge the basis for his employment termination, it raises a risk of vulnerability, so AG ¶ 16(e) applies.

His 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"). The company investigator learned that Applicant had viewed inappropriate adult images on his work computer by use of an investigative search tool on the computer itself and not from Applicant. More than two years have passed since Applicant's misuse of his work computer was discovered, but his knowing disregard of his company's policies prohibiting unauthorized use of a government-owned asset, and his breach of his obligation to his employer to cooperate with the investigation, cannot reasonably be characterized as minor offenses mitigated under ¶ 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").

Applicant has acknowledged that he made bad judgments ("I was maybe in middle age crisis or whatever, but it happened"), including that he violated the trust of his spouse by viewing the sexual images at work (Tr. 32-33). Applicant made changes to prevent recurrence of his misuse of a computer by putting his personal computer in the open and educating himself about his ethical responsibilities to his current employer. Concerning his falsification, he disclosed on his e-QIP that he had been fired in May 2005 for inadvertently copying files of a personal nature, "including files that were considered pornographic," onto the server at work, and that he had not been as open as he should have been during the investigation. He expressed regret at not being as forthright as he should have been. However, 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") applies only in part.

As persuasively argued by the government, Applicant has not adequately explained what led him to view sexual images at work in the first place. He has not obtained any counseling, so it is not clear whether the factors that led to the behavior are not going to recur. More troubling is Applicant's characterization of his conduct as "a single issue" and as "a one time mistake." (*See* Answer). While the loading of the improper adult material on the server occurred one time and was unintentional, he viewed sexual images on his work computer intermittently. In response to SOR ¶ 1.b, Applicant indicated, "I never intentionally misused the computer and loading the files was an accident." Applicant did not realize that previously viewed images remained automatically cached on his workstation computer, but it is not accurate for him to maintain that he never intentionally misused the computer since he knew he had viewed sexual images off his jazz drive at work on the government-owned computer monitor. The ethics courses Applicant took at work have yet to impress upon him the obligation of full candor.

Furthermore, AG ¶ 17(e) ("the individual has taken positive steps to reduce or eliminate vulnerability to exploitation, manipulation, or duress") applies only in part. Although Applicant claims he would divulge the circumstances surrounding his termination if he had to, and his spouse would support him in that regard, his employer is still unaware that he left his previous job under unfavorable circumstances. It is not clear whether the security office at work viewed his completed e-QIP before or after he submitted it, which would have gone a long way towards eliminating the vulnerability concerns raised by his concealment of his job firing from his present employer.

Guideline M—Use of Information Technology Systems

The security concern related to the guideline 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.

As discussed under Guideline E, *supra*, Applicant violated his employer's polices concerning authorized use of a government-owned information resource asset when he improperly and repeatedly viewed adult images using his work computer in 2005 if not before,[5] and on that occasion in April 2005 when he inadvertently, but negligently loaded sexually explicit images onto a national laboratory's server. AG ¶ 40(e) ("unauthorized use of a government or other information technology system") and ¶ 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.

There is no evidence of any misuse of a work computer by Applicant since he started with his present employer in October 2005. Yet, Applicant has not shown that "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." (AG ¶ 41(a)). His knowing disregard of policies prohibiting unauthorized use continues to cast doubt about his personal judgment, notwithstanding the passage of almost three years since his conduct was discovered in April 2005. He made no showing that his viewing of sexually explicit images was unusual, even at work.

In the absence of any evidence that Applicant's posting of sexually explicit images on the server was other than an isolated mistake, mitigating condition 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") applies, but only in part. Once he was informed of the titles of the sexually explicit material on the server, Applicant acknowledged it was his and that he must have loaded it by mistake. Not all of the JPEG/MPEG files on his computer matched those loaded onto the server, and his viewing/maintaining sexually explicit material on the computer is not mitigated under AG ¶ 41(c). As discussed *supra*, the steps Applicant has taken to preclude a

[5]Applicant was asked how many times he had brought the jazz drive containing sexually explicit images to work and he testified, "A lot" (Tr. 71), all after his marriage to his current wife.

recurrence do not completely mitigate this knowing and repeated disregard of company policy concerning the use of a government-owned information resource.

I have evaluated Applicant's conduct under the whole person concept, applying the conclusions set forth previously in this analysis. Applicant's work performance for his current employer has been outstanding. Yet, while he claims he learned a "hard lesson" and paid a high price for his mistakes, including his failure to be "fully straight out" with the government investigator (Tr. 39-40), I am unable to conclude under the totality of the facts and circumstances that it is clearly consistent with the national interest to grant him a security clearance. He has not been fully forthcoming with his employer about his firing from his previous job, or with the Department of Defense about the extent of his misuse of the work computer when he answered the SOR. Even at his hearing, he was reluctant to take responsibility for misuse of the computer to view the pornography on his personal portable drive. A "mid-life crisis" does not adequately explain what led him to violate his employer's policies concerning the use of the work computer.

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 E:	AGAINST APPLICANT
Subparagraph 1.a:	For Applicant
Subparagraph 1.b:	Against Applicant
Subparagraph 1.c:	For Applicant
Subparagraph 1.d:	Against Applicant
Subparagraph 1.e:	Against Applicant[6]
Paragraph 2, Guideline M:	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

[6]Applicant's employment termination does not represent additional misconduct, but is merely the consequences of his knowing violation of company policies and his effort to cover it up.