DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
----------	)	ISCR Case No. 07-10583
SSN: ----------	)	
	)	
Applicant for Security Clearance	)	

Appearances

For Government: John B. Glendon, Esquire, Department Counsel
Tovah Minster, Esquire, Department Counsel
For Applicant: *Pro Se*

June 22, 2009

_____

Decision

_____

HARVEY, Mark, Administrative Judge:

In the 1990s, Applicant downloaded approximately 500 pornographic images on his government-issued computers, while employed in a sensitive, important government position. In 2008 he made two statements, in which he denied that he used his government computer to view pornography. Applicant mitigated the security concern about his misuse of a government information technology system because this misuse was not recent and is unlikely to recur. However, he failed to mitigate personal conduct security concerns related to making false statements in 2008. Eligibility for access to classified information is denied.

Statement of the Case

On September 7, 2005, Applicant submitted an Electronic Questionnaires for Investigations Processing (e-QIP) or Security Clearance Application (SF 86) (Government Exhibit (GE) 1). On March 12, 2009, the Defense Office of Hearings and Appeals (DOHA) issued a statement of reasons (SOR) to Applicant, pursuant to Executive Order 10865, *Safeguarding Classified Information Within Industry,* dated February 20, 1960, as amended and modified, and Department of Defense Directive

5220.6, *Defense Industrial Personnel Security Clearance Review Program* (Directive), dated January 2, 1992, as amended and modified. The revised adjudicative guidelines (AG) promulgated by the President on December 29, 2005, are effective within the Department of Defense for SORs issued after September 1, 2006.

The SOR alleges security concerns under Guidelines E (Personal Conduct) and M (Use of Information Technology Systems). The SOR detailed reasons why DOHA could not make the preliminary affirmative finding under the Directive that it is clearly consistent with the national interest to grant or continue a security clearance for Applicant, and recommended referral to an administrative judge to determine whether Applicant's clearance should be granted, continued, denied, or revoked.

On March 23, 2009, Applicant responded to the SOR allegations, and requested a hearing before an administrative judge (GE 7). Department Counsel was prepared to proceed on May 5, 2009. On May 7, 2009, the case was assigned to an administrative judge. On May 13, 2009, DOHA issued a hearing notice (GE 5). Due to a family emergency, the case was transferred to me on June 2, 2009 (Transcript (Tr.) 4-5). The hearing was held on June 3, 2009. Department Counsel offered four exhibits (GE 1-4) (Tr. 20-21), and Applicant offered two exhibits (Tr. 23-25, 40-41; Applicant Exhibits (AE) A-B). There were no objections, and I admitted GE 1-4 (Tr. 21) and AE A-B (Tr. 25-26, 41). Additionally, I admitted the Notice of Hearing, SOR, and response to the SOR (GE 5-7). I received the transcript on June 11, 2009.

Findings of Fact[1]

In Applicant's response to the SOR, Applicant admitted all of the SOR allegations, except he expressed some skepticism about the number of pornographic images found on his computer and the number of government computers found to contain pornographic images (GE 7). His admissions are accepted as findings of fact. After a complete and thorough review of the evidence of record, I make the following findings of fact.

Applicant is between 70 and 80 years old (Tr. 6). He graduated from a service academy about 50 years ago (Tr. 26). He served on active duty for about 35 years and retired in the 1990s (Tr. 26). His retirement grade was at the two-star level. His retirement award was the Distinguished Service Medal (AE A at 8). The service chief in Applicant's branch of service presided at his retirement ceremony (AE A at 8). During his career, he received eight Legion of Merit Medals (GE A at 9). He commanded a vast organization with enormous fire power, including nuclear weapons (GE A at 9-10). He supervised a budget of over $2 billion (AE A at 7). He has had an extraordinary career of service and made tremendous contributions to the national defense of the United

[1]Some details have not been included in order to protect Applicant's right to privacy because this decision after minimal redaction will be posted on the internet. Specific information is available in the cited transcript and exhibits.

States (AE A). At various times during his career, Applicant has held a top secret clearance with access to sensitive compartmented information (Tr. 36; AE A).

Applicant has been married for more than 40 years. He has several children and grandchildren (Tr. 26-27; AE B at 3). After retirement from active service, he worked for a defense contractor in relation to foreign military sales (Tr. 28). In the 1990s, he worked at a very high level in the government, in an extremely sensitive position for about a year, and then returned to the private sector (Tr. 28). He currently works as a consultant to the government, as a program manager for an entity that is closely associated with the government, and is on the board of directors for a government contractor (Tr. 29-31).

Misuse of government computers[2]

For about one year in the 1990s, Applicant was employed in an extremely sensitive government position. Use of his government computer while on duty to view images of adults engaged in pornographic activities, while occupying this position, would cast significant discredit upon the Department of Defense and it violates rules in his workplace about use of his government computer and on-duty Internet use.

In the 1990s, while employed in this sensitive position, Applicant noticed his computer was operating slowly or had difficulties with its dial-up connection. Applicant asked computer maintenance to take corrective action. Maintenance replaced his computer with another government computer. Maintenance personnel discovered numerous Graphics Interface Format (.gif) files depicting individuals involved in sexual activity. Forensic computer analysts found 379 graphic images of adults engaged in pornographic activities on one hard drive (ROI ¶ 3-9). About a month later, investigators obtained the hard drive from his replacement computer and discovered 210 graphic images of adult pornography (ROI ¶ 3-6). A total of about 80 files found on the two hard drives were recovered from deleted files. The forensic examination of the two hard drives did not indicate how many files were automatically saved by the computer in temporary files and whether any files discovered on his computer were deliberately saved by Applicant and placed into folders for subsequent viewing.[3]

Two images found on his hard drive depicted nude prepubescent adolescents (ROI ¶ 3-16a). One of the images was of very poor quality. Applicant denied that he had searched the internet for any child pornography (Tr. 39). He denied knowingly opening

[2] Unless stated otherwise, the facts in this section are from a Report of Investigation (ROI) completed in the 1990s (Applicant was titled as the SUBJECT of the investigation) (GE 2).

[3] It is possible from the way the ROI was written that three computer hard drives were forensically examined and about 800 images of adult pornography were found (SOR ¶¶ 1.a to 1.c). The more credible interpretation is that the government evaluated two computer hard drives and found 500-600 images of pornography. Applicant thought the number of images alleged in the SOR might be an exaggeration; however, he conceded whether it was 500 images or 800 images was not a significant issue (Tr. 60-61; GE 7).

any .gif files showing child pornography (Tr. 39). He denied that he had any sexual interest whatsoever in children or viewing nude or sexual images of children (Tr. 39).

The military investigators turned the investigation was turned over to the Federal Bureau of Investigation after he ended his federal employment in the late 1990s. Applicant was never questioned or confronted about misuse of his government computer (ROI ¶ 3-32 and ROI cover letter; Tr. 45). Applicant was not advised of the existence of the investigation until 2009. Applicant told his spouse about the investigation shortly after he was advised of its results (Tr. 59).

After leaving government service in the 1990s, Applicant occasionally viewed pornography (Tr. 60). He described his contact with internet pornography over the last ten years as "infrequent" (Tr. 60). Applicant downloaded and viewed some images of adults engaged in pornographic activities while on duty at his government place of employment.

Falsification of security clearance related documentation

On April 28, 2008, an Office of Personnel Management (OPM) investigator questioned Applicant about his misuse of a government computer to search for and look at pornographic material (Tr. 49). Applicant orally responded, "no, certainly not," when he was confronted with the allegations (Tr. 49). Applicant provided an affidavit, which states, "I never misused a government computer and do not view child pornography" (GE 3). Applicant signed the statement and knew the part about denying that he viewed images of adults engaged in pornographic activities was not true at the time he made this statement (Tr. 53-54).

On September 25, 2008, Applicant responded to a DOHA interrogatory, "To my knowledge I have not used any work computer to view pornographic material at [my government office]. In fact, I have thought all such computers blocked access to such sites. If I did so, it must have been very isolated as I don't have time to surf the Internet in any of my jobs." (Tr. 52-53; GE 4). Applicant signed this statement and knew it was not true at the time he made this statement (Tr. 56-58).

At his hearing Applicant stated, "When I was presented with the first round of these allegations, I hotly and falsely denied same, both orally and subsequently, meaning later, on in the hour, in a statement that I submitted to the government representative" (Tr. 42). He vigorously denied that he viewed images of adults engaged in pornographic activities to the OPM investigator. At his hearing, he described himself as being "blatantly" untruthful when he denied viewing images of adults engaged in pornographic activities (Tr. 50-51). Applicant had extraordinary regret about his actions (Tr. 56). He acknowledged in his SOR response and reiterated at his hearing that his responses to the OPM investigator and to the DOHA interrogatory were false in regard to his claim that he did not view images of adults engaged in pornographic activities on his government computer (Tr. 58).

Applicant conceded that the government should have a higher expectation of honesty and integrity for him because of his age and experience (Tr. 45). He emphasized that he did not knowingly view any child pornography and he did not recall ever seeing the two images of child pornography cited in the ROI (AE B at 2).[4] He described his mental state in 2008 when he denied viewing images of adults engaged in pornographic activities on his government computer as "a combination of haughtiness, fear and embarrassment." (AE B at 2).

Policies

The U.S. Supreme Court has recognized the substantial discretion of the Executive Branch in regulating access to information pertaining to national security emphasizing, "no one has a 'right' to a security clearance." *Department of the Navy v. Egan*, 484 U.S. 518, 528 (1988). As Commander in Chief, the President has the authority to control access to information bearing on national security and to determine whether an individual is sufficiently trustworthy to have access to such information." *Id*. at 527. The President has authorized the Secretary of Defense or his designee to grant Applicant's eligibility for access to classified information "only upon a finding that it is clearly consistent with the national interest to do so." Exec. Or. 10865, *Safeguarding Classified Information within Industry* § 2 (Feb. 20, 1960), as amended and modified.

Eligibility for a security clearance is predicated upon the Applicant meeting the criteria contained in the revised adjudicative guidelines (AG). These guidelines are not inflexible rules of law. Instead, recognizing the complexities of human behavior, these guidelines are applied in conjunction with an evaluation of the whole person. An administrative judge's over-arching adjudicative goal is a fair, impartial and common sense decision. An administrative judge must consider all available, reliable information about the person, past and present, favorable and unfavorable.

The government reposes a high degree of trust and confidence in persons with access to classified information. This relationship transcends normal duty hours and endures throughout off-duty hours. 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. Clearance decisions must be "in terms of the national interest and shall in no sense be a determination as to the loyalty of the [A]pplicant concerned." *See* Exec. Or. 10865 § 7. *See also* Executive Order 12968 (Aug. 2, 1995), Section 3. Thus, nothing in this Decision should be construed to suggest that I have based this decision, in whole or in part, on any express or implied determination as to Applicant's allegiance, loyalty, or patriotism. It is merely an indication the Applicant has not met the strict guidelines the President and the Secretary of Defense have established for issuing a clearance.

[4] The SOR did not allege that he viewed or possessed any images of child pornography (GE 6). The only information about the two images of child pornography was contained in the ROI (GE 2).

Initially, the government must establish, by substantial evidence, conditions in the personal or professional history of the Applicant that may disqualify the Applicant from being eligible for access to classified information. The government has the burden of establishing controverted facts alleged in the SOR. *See Egan*, 484 U.S. at 531. "Substantial evidence" is "more than a scintilla but less than a preponderance." *See v. Washington Metro. Area Transit Auth.*, 36 F.3d 375, 380 (4th Cir. 1994). The guidelines presume a nexus or rational connection between proven conduct under any of the criteria listed therein and an Applicant's security suitability. *See* ISCR Case No. 95-0611 at 2 (App. Bd. May 2, 1996).

Once the government establishes a disqualifying condition by substantial evidence, the burden shifts to the Applicant to rebut, explain, extenuate, or mitigate the facts. Directive ¶ E3.1.15. An Applicant "has the ultimate burden of demonstrating that it is clearly consistent with the national interest to grant or continue his security clearance." ISCR Case No. 01-20700 at 3 (App. Bd. Dec. 19, 2002). The burden of disproving a mitigating condition never shifts to the government. *See* ISCR Case No. 02-31154 at 5 (App. Bd. Sep. 22, 2005). "[S]ecurity clearance determinations should err, if they must, on the side of denials." *Egan*, 484 U.S. at 531; *see* AG ¶ 2(b).

Analysis

Upon consideration of all the facts in evidence, and after application of all appropriate legal precepts, factors, and conditions, I conclude the relevant security concerns are under Guidelines E (Personal Conduct) and M (Use of Information Technology Systems).

Personal Conduct

AG ¶ 15 expresses the security concern pertaining to personal conduct:

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

AG ¶ 16 describes two conditions that could raise a security concern and may be disqualifying in this case:

> (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; and

(b) deliberately providing false or misleading information concerning relevant facts to an employer, investigator, security official, competent medical authority, or other official government representative.

On April 28, 2008, Applicant falsely denied using his government computer to view images of adults engaged in pornographic activities to an OPM investigator and on September 25, 2008, he reiterated this false denial in response to DOHA interrogatories. However, he admitted in his SOR response and at his hearing that his answers on these two previous occasions about viewing images of adults engaged in pornographic activities were false. AG ¶¶ 16(a) and 16(b) both apply.

AG ¶ 17 provides seven conditions that could mitigate personal conduct security concerns in this case:

(a) the individual made prompt, good-faith efforts to correct the omission, concealment, or falsification before being confronted with the facts;

(b) the refusal or failure to cooperate, omission, or concealment was caused or significantly contributed to by improper or inadequate advice of authorized personnel or legal counsel advising or instructing the individual specifically concerning the security clearance process. Upon being made aware of the requirement to cooperate or provide the information, the individual cooperated fully and truthfully;

(c) the offense is so minor, or so much time has passed, or the behavior is so infrequent, or it happened under such unique circumstances that it is unlikely to recur and does not cast doubt on the individual's reliability, trustworthiness, or good judgment;

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

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

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

(g) association with persons involved in criminal activity has ceased or occurs under circumstances that do not cast doubt upon the individual's reliability, trustworthiness, judgment, or willingness to comply with rules and regulations.

None of the mitigating conditions apply. The falsification is established. He admitted that he deliberately and intentionally provided false information on two

occasions when he denied that he viewed images of adults engaged in pornographic activities in the context of a review to decide whether his security clearance should be continued.[5]

Use of Information Technology Systems

AG ¶ 39 articulates the security concern relating to misuse of information technology systems:

> 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.

AG ¶¶ 40(e) and 40(f) detail two conditions that could raise a security concern and may be disqualifying in this case. AG 40(e) states, "unauthorized use of a government or other information technology system," and AG ¶ 40(f) provides, "introduction, removal, or duplication of hardware, firmware, software, or media to or from any information technology system without authorization, when prohibited by rules, procedures, guidelines or regulations." Applicant was well aware that he was not authorized to use a government computer to access and download files depicting pornographic images onto his government computer. By viewing .gif files on Internet sites showing images of adults engaged in pornographic activities, he automatically downloaded or introduced those media-images or .gif files onto his computer hard drive. As such, his introduction of those images onto his computer was probably unintentional because he was not aware that they would be automatically downloaded onto his computer. However, other pornographic .gif files were evidently intentionally saved or introduced onto his computer hard drive and then subsequently deleted from his computer hard drive. The forensic investigator then recovered the deleted .gif files, establishing by substantial evidence their previous intentional, unauthorized introduction

[5]The Appeal Board has cogently explained the process for analyzing falsification cases, stating:

> (a) when a falsification allegation is controverted, Department Counsel has the burden of proving falsification; (b) proof of an omission, standing alone, does not establish or prove an applicant's intent or state of mind when the omission occurred; and (c) a Judge must consider the record evidence as a whole to determine whether there is direct or circumstantial evidence concerning the applicant's intent or state of mind at the time the omission occurred. [Moreover], it was legally permissible for the Judge to conclude Department Counsel had established a prima facie case under Guideline E and the burden of persuasion had shifted to the applicant to present evidence to explain the omission.

ISCR Case No. 03-10380 at 5 (App. Bd. Jan. 6, 2006) (citing ISCR Case No. 02-23133 (App. Bd. June 9, 2004)). In this case, Applicant did not contest the allegations of falsification.

onto his computer hard drive. AG ¶¶ 40(e) and 40(f) both apply and further inquiry and analysis about the applicability of mitigating conditions is necessary.

AG ¶ 41 provides three mitigating conditions that could mitigate security concerns including:

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

AG ¶ 41(a) fully applies and AG ¶¶ 41(b) and 41(c) do not apply. Applicant downloaded about 500 images of adults engaged in pornographic activities. His conduct in going to the sexually-explicit Internet sites, and opening these .gif files was not accidental, unintentional or inadvertent. He knew when he double clicked these icons the type of image that would be revealed. This conduct was not done for organizational efficiency or effectiveness. He did not admit this conduct until after he was advised that he had been investigated for it. As such, his admissions were not spontaneous.

However, Applicant's abuse of government computers occurred more than 10 years ago. He does not currently use a government computer, and has not been a government employee for at least 10 years. His viewing of adult pornography (which is not connected to his government service as a contractor) is private and infrequent. His viewing of images of adults engaged in pornographic activities using his government-issued computer, while on duty as a government employee in the 1990s under all the facts and circumstances, "does not cast doubt on [his current] reliability, trustworthiness, or good judgment." Security concerns pertaining to use of information technology systems are mitigated. *See* AG ¶ 41(a).

Whole Person Concept

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

> (1) the nature, extent, and seriousness of the conduct; (2) the circumstances surrounding the conduct, to include knowledgeable

participation; (3) the frequency and recency of the conduct; (4) the individual's age and maturity at the time of the conduct; (5) the extent to which participation is voluntary; (6) the presence or absence of rehabilitation and other permanent behavioral changes; (7) the motivation for the conduct; (8) the potential for pressure, coercion, exploitation, or duress; and (9) the likelihood of continuation or recurrence.

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. AG ¶ 2(c). I have incorporated my comments under Guidelines E and M in my whole person analysis. Some of the factors in AG ¶ 2(a) were addressed under that guideline, but some warrant additional comment.

Although the rationale for reinstating Applicant's clearance is insufficient to support a security clearance at this time, there are several factors that support approval of his clearance. During his active service from the 1950s to the 1990s, he received the Distinguished Service Medal and eight Legion of Merit awards. The service chief of Applicant's branch of service presided at his retirement ceremony in the 1990s. Applicant deserves substantial credit for volunteering to support his service and the Department of Defense thereafter for about 50 years. He has served his nation and the national defense extraordinarily well, rising to very high level on active duty and subsequently in a civil capacity. His longevity and success speaks very well for his dedication, patriotism and loyalty to the United States, the U.S. government, and his employer. There were no allegations of security violations. He does not abuse alcohol or illegal drugs. He made mistakes, and he admitted them in his SOR response and at his hearing. I specifically find his denial of intentionally viewing or ever intending to view any child pornography to be credible. His remorse about viewing the adult pornography on his government computer and about making false statements about that misconduct in April and September 2008 is heartfelt and sincere. He has learned from his mistakes and I am confident that he will not repeat them. These factors show substantial responsibility, rehabilitation, and mitigation.

The whole person factors against reinstatement of Applicant's clearance are more substantial at this time. Making false statements to an OPM investigator and in response to a DOHA interrogatory is not prudent or responsible. He had ample opportunity between being confronted by the OPM investigator on April 28, 2008, and receipt of the DOHA interrogatories on September 25, 2008, to correct the false information he provided to the government. Instead on September 25, 2008, he submitted more false information to the government. Notwithstanding his truly extraordinary background and contributions to the nation, his two falsifications are recent, material, and cannot be mitigated at this time.

After weighing the disqualifying and mitigating conditions, and all the facts and circumstances, in the context of the whole person, I conclude Applicant has not mitigated the personal conduct security concerns. I take this position based on the law, as set forth in *Department of Navy v. Egan,* 484 U.S. 518 (1988), my careful consideration of the whole person factors and supporting evidence, my application of

the pertinent factors under the Adjudicative Process, and my interpretation of my responsibilities under the Guidelines. Applicant has failed to mitigate and/or overcome the government's case. For the reasons stated, I conclude he is not eligible for access to classified information.

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
Subparagraphs 1.a to 1.c:	For Applicant
Subparagraphs 1.d and 1.e:	Against Applicant
Paragraph 2, Guideline M:	For Applicant
Subparagraph 2.a:	For Applicant

Conclusion

In light of all the circumstances presented by the record in this case, it is not clearly consistent with the national interest to grant or continue Applicant's eligibility for a security clearance. Eligibility for a security clearance is denied.

_____
MARK HARVEY
Administrative Judge