DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
----------	)	ISCR Case No. 08-08631
SSN: ----------	)	
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Pamela C. Benson, Esquire, Department Counsel
For Applicant: *Pro Se*

February 24, 2010

Decision

HOWE, Philip S., Administrative Judge:

On January 16, 2008, Applicant submitted his electronic Security Clearance Application (SF 86) (e-QIP). On June 28, 2009, the Defense Office of Hearings and Appeals (DOHA) issued Applicant a Statement of Reasons (SOR) detailing security concerns under Guidelines D (Sexual Behavior), E (Personal Conduct), M (Use of Information Technology Systems), and J (Criminal 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 within the Department of Defense for SORs issued after September 1, 2006.

Applicant acknowledged receipt of the SOR on June 30, 2009. He answered the SOR in writing on July 7, 2009, and requested a hearing before an administrative judge. DOHA received the request on July 13, 2009. Department Counsel was prepared to proceed on July 21, 2009, and I received the case assignment on August 27, 2009.

DOHA issued a Notice of Hearing on October 29, 2009, and I convened the hearing as scheduled on November 18, 2009. The Government offered Exhibits 1 through 8, which were received without objection, except for Exhibit 4. I considered the objection and overruled it, admitting the exhibit into evidence. Applicant testified. He submitted Exhibits A and B, which were admitted without objection. (Tr. 53, 54) DOHA received the transcript of the hearing (Tr.) on December 1, 2009. Based upon a review of the case file, pleadings, exhibits, and testimony, eligibility for access to classified information is denied.

Procedural and Evidentiary Rulings

Motion to Amend SOR

Department Counsel moved to amend the SOR by adding to ¶ 1.b, after "images of" the words, "nude and/or sexually explicit." Applicant objected on the basis the government originally could have written the allegation that way but failed to do so. I overruled the objection and allowed the amendment because it was a clarifying amendment within the context of the existing allegations. (Tr. 8-11)

Findings of Fact

In his Answer to the SOR, dated July 7, 2009, Applicant denied the factual allegations in all paragraphs of the SOR. He also provided additional information to support his request for eligibility for a security clearance.

Applicant is 39 years old, married for 14 years, and has three children. He works for a defense contractor. He started that job in November 2007. He currently has a security clearance and has had a clearance since 2001. (Tr. 55-58; Exhibit 1)

Applicant worked for another defense contractor from November 2005 until October 25, 2007, a Thursday. On that day, the employer terminated Applicant for cause. He is not eligible for rehiring by the company. The reason for termination was the use of his employer's computer to access child pornography websites on the internet during work hours. The employer installed software on its computers on October 19, 2007, to track any employee's access to the internet. Applicant was identified as one of those employees accessing pornographic websites during work hours. The company software discovered Applicant went to the child pornography website 14 times between 0920 and 0924 on October 22, 2007, using the company computer, and downloaded onto his company computer numerous pictures of nude and/or sexually explicit young pre-teen and teenage boys. (Tr. 24-39, 57, Exhibit 2 to 6)

The company shipped the hard drive from Applicant's computer to their headquarters for examination by the local police forensic unit. The police department discovered child pornographic images on Applicant's hard drive. The police department also discovered that Applicant had installed Lime Wire on his hard drive. He made this installation without authority or permission from his employer. This software is used to

share downloaded images, including those of child pornography. The police sent the recovered child pornographic images to the National Center for Missing and Exploited Children (NCMEC) for identification purposes. The NCMEC identified 22 images as known child pornographic images. The police department report is dated November 29, 2007. (Tr. 24-39; Exhibits 2-5)

A company vice-president testified that he was Applicant's supervisor. The vice-president has worked in government contracting for 44 years and has had a security clearance for many of those years. Applicant used a company computer at work. The company had a policy against excessive internet use of the computer not related to company work. The company had problems with employees engaging in such usage for considerable periods of time. After the installation of computer monitoring software on Friday October 19, 2007, the company identified six employees at the vice-president's work location who were using the internet excessively. One of those persons identified was Applicant, who worked in the vice-president's division, as the security officer and safety officer. All six persons were terminated. The vice-president obtained information from the computer staff about Applicant's internet use during the work day. He was informed that Applicant was looking at child pornography sites and was sometimes spending up to six hours a day on the internet. The vice-president told Applicant that he was terminated and had to depart the building immediately with his personal items or return the following day to get his property while being escorted in the building. He made it clear to Applicant that he was fired from the job and for what reason. Applicant's company badge was taken from him at that time. Applicant was not eligible for rehiring. He did not tell Applicant he was "laid off." Later that day, Applicant's computer was dismantled and the hard drive was sent to the company headquarters. The vice-president described Applicant as an average employee and somewhat dedicated to his work. (Tr. 24-39, 43, 45, 46, 63, 71, 72; Exhibits 6-8)

Applicant applied for unemployment compensation and obtained it after his termination. He was paid for one month. Under the applicable state law, a former employer may contest the awarding of unemployment compensation. This employer, according to the vice-president, usually does not oppose the unemployment compensation and did not do so in this case. (Tr. 38-40, 76, 77, 80; Exhibit 7)

Applicant denied he downloaded the pornographic pictures onto his office computer. He claimed it was a hand-me-down computer which the company placed in his office. He used a laptop computer for other business purposes. Applicant testified that his office computer was used by new applicants for company jobs to complete their security applications. The job applicants would do research on the computer to be able to complete the applications. He did not monitor their activities, but only answered their questions. He does not know how the pornographic pictures appeared on his company computer. (Tr. 59-66)

Applicant denies installing computer software named "Lime wire" on his company computer. He claims his computer was a "hand-me-down" computer and he was the

third user. Applicant denies all wrongdoing regarding his computer and internet access as alleged in the SOR. (Tr. 78-98, 101-104)

Applicant completed his e-QIP on January 16, 2008. He answered Question 22 regarding being fired from a job in the past seven years, quitting a job after being told he would be fired, departed a job following allegations of misconduct, or by mutual agreement after allegations of unsatisfactory performance, or for any other reason under unfavorable circumstances with a negative reply. Applicant did not disclose the October 25, 2007, termination from his former employer. He considered himself "released" not terminated. Applicant testified that he did not learn of the reasons for his termination until 2008. (Tr. 66-75, 94; Exhibit 8)

Applicant submitted three character statements as part of his Answer. He also submitted his checking account statement from November 2007 showing the unemployment compensation deposits. The character statements present Applicant as responsible and well-organized, an excellent security officer, and helpful in organizing an open house in 2008 at his work place. (Tr. 98, 99; Answer)

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, an "applicant is responsible for presenting witnesses and other evidence to rebut, explain, extenuate, or

mitigate facts admitted by applicant or proven by Department Counsel, and has the ultimate burden of persuasion as to obtaining a favorable clearance 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 D, Sexual Behavior

AG ¶ 12 expresses the security concern under this guideline:

> Sexual behavior that involves a criminal offense, indicates a personality or emotional disorder, reflects lack of judgment or discretion, or which may subject the individual to undue influence or coercion, exploitation, or duress can raise questions about an individual's reliability, trustworthiness and ability to protect classified information. No adverse inference concerning the standards in this Guideline may be raised solely on the basis of the sexual orientation of the individual.

AG ¶ 13 describes four conditions that could raise a security concern and may be disqualifying. All of them are applicable here:

> (a) sexual behavior of a criminal nature, whether or not the individual has been prosecuted;
>
> (b) a pattern of compulsive, self-destructive, or high risk sexual behavior that the person is unable to stop or that may be symptomatic of a personality disorder;
>
> (c) sexual behavior that causes an individual to be vulnerable to coercion, exploitation, or duress; and

(d) sexual behavior of a public nature and/or that reflects lack of discretion or judgment.

Applicant spent up to six hours daily looking at pornographic websites on his company's computer between October 22 and 25, 2007. This action was contrary to company policy. The government's exhibits and the testimony of the company official are very credible on this issue. Viewing child pornography and downloading it to a computer is contrary to law and policy. AG ¶ 13 (a) applies.

The frequency of Applicant's actions shows a pattern of compulsive and self-destructive sexual behavior. He was not able to stop his actions. AG ¶ 13 (b) applies.

Applicant's behavior makes him vulnerable to coercion, exploitation, or duress, if known to the public. Applicant does not want to be known as a husband and father who views child pornography at work sites. AG ¶ 13 (c) applies. Applicant's actions show a lack of discretion or judgment. AG ¶ 13 (d) applies.

AG ¶ 14 provides conditions that could mitigate security concerns. None of these mitigating conditions apply on the facts presented by Applicant:

(a) the behavior occurred prior to or during adolescence and there is no evidence of subsequent conduct of a similar nature;

(b) the sexual behavior happened so long ago, so infrequently, or under such unusual circumstances, that it is unlikely to recur and does not cast doubt on the individual's current reliability, trustworthiness, or good judgment;

(c) the behavior no longer serves as a basis for coercion, exploitation, or duress; and,

(d) the sexual behavior is strictly private, consensual, and discreet.

Applicant's general denials of any misconduct and inappropriate use of the company computer is not credible or persuasive. He offers no concrete evidence that any of these mitigating conditions apply.

Guideline E, 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.

The following will normally result in an unfavorable clearance action or administrative termination of further processing for clearance eligibility:

(a) refusal, or failure without reasonable cause, to undergo or cooperate with security processing, including but not limited to meeting with a security investigator for subject interview, completing security forms or releases, and cooperation with medical or psychological evaluation; and,

(b) refusal to provide full, frank and truthful answers to lawful questions of investigators, security officials, or other official representatives in connection with a personnel security or trustworthiness determination.

AG ¶ 16 describes seven conditions that could raise a security concern and may be disqualifying. One condition applies because of the allegation of failure to answer the question truthfully on the e-QIP pertaining to his job loss in the past seven years:

(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.

Applicant did not disclose in answering Question 22 of the e-QIP that he had been terminated on October 25, 2007, by his employer. This condition applies.

AG ¶ 17 provides seven conditions that could mitigate security concerns:

(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.

Under the evidence Applicant introduced at the hearing none of the mitigating conditions apply. Applicant denies he was terminated, only "released" from work by his employer. He also contends his receipt of unemployment compensation after his termination is determinative of the issue that he was not terminated. The testimony of the company vice-president was conclusive on this aspect of the event. The company for which Applicant worked does not usually contest unemployment compensation claims. Applicant only received compensation for one month before he obtained another job.

Guideline M, Use of Information Technology Systems

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

Noncompliance with rules, procedures, guidelines or regulations pertaining to information technology systems may raise security concerns about an individual's 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 describes eight conditions that could raise a security concern and may be disqualifying. Four conditions apply in this case:

(a) illegal or unauthorized entry into any information technology system or component thereof;

(b) illegal or unauthorized modification, destruction, manipulation or denial of access to information, software, firmware, or hardware in an information technology system;

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

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

Applicant used his company's computer to illegally access child pornography websites, and other sexually explicit material, during work hours in violation of company policy. He installed "Lime ware" file sharing software on his computer's hard drive without authority from his company. Each of these four disqualifying conditions applies because of the modifications Applicant made without authority to his company's computer that was assigned to him, as well as his subsequent actions on the computer.

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

(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.

None of these mitigating conditions apply to Applicant's situation. His behavior is recent, deliberate, not minor, and done for his own gratification and benefit. Applicant made no effort to correct the situation. His general and repeated denials are not persuasive. There is no counseling or rehabilitation shown, hence no evidence that similar conduct is unlikely to recur.

Guideline J, Criminal Conduct

AG ¶ 30 expresses the security concern pertaining to criminal conduct:

> Criminal activity creates doubt about a person's judgment, reliability, and trustworthiness. By its very nature, it calls into question a person's ability or willingness to comply with laws, rules and regulations.

AG ¶ 31 describes five conditions that could raise a security concern and may be disqualifying. Two conditions apply:

> (a) a single serious crime or multiple lesser offenses; and
>
> (c) allegation or admission of criminal conduct, regardless of whether the person was formally charged, formally prosecuted or convicted.

Applicant illegally viewed pornographic websites and downloaded numerous images of nude and/or sexually explicit photographs of young pre-teen and teenage boys onto his company computer during work days. Such viewing and downloading over four days in October 2007 are repeated criminal actions. Applicant was never indicted or tried in criminal court for his alleged actions. But he did not have to be convicted of the allegations for the disqualifying condition to apply.

AG ¶ 32 provides four conditions that could mitigate security concerns:

> (a) so much time has elapsed since the criminal 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 person was pressured or coerced into committing the act and those pressures are no longer present in the person's life;
>
> (c) evidence that the person did not commit the offense; and
>
> (d) there is evidence of successful rehabilitation; including but not limited to the passage of time without recurrence of criminal activity, remorse or restitution, job training or higher education, good employment record, or constructive community involvement.

None of them apply. The time since Applicant used his company computer to access the sex sites is comparatively recent. Applicant was not pressured into looking at these sites. He did commit the actions. Applicant denies any of the access activities, so there is no rehabilitation if the Applicant does not acknowledge the misbehavior.

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 an 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.

AG ¶ 2(c) requires each case must be judged on its own merits. Under AG ¶ 2(c), the ultimate determination of whether to grant eligibility for a security clearance must be an overall commonsense judgment based upon careful consideration of the guidelines and the whole-person concept.

I considered the potentially disqualifying and mitigating conditions in light of all the facts and circumstances surrounding this case. Applicant was an adult, husband, and father when he accessed pornographic sites from his office computer. He denies anything wrong ever occurred, or that he was terminated for misconduct by his employer in October 2007. He accessed the sites daily. There is no evidence Applicant showed that he underwent any rehabilitation for viewing child pornography because he denies he ever accessed the pornography. His denials are not credible when compared to the detailed documents and testimony presented documenting his misconduct.

Overall, the record evidence leaves me with questions and doubts as to Applicant's eligibility and suitability for a security clearance. For all these reasons, I conclude Applicant did not mitigate the security concerns arising from his sexual behavior, personal conduct, information technology systems use, and criminal conduct. I conclude the "whole-person" concept against Applicant.

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 D:	AGAINST APPLICANT
Subparagraph 1.a:	Against Applicant
Subparagraph 1.b:	Against Applicant

Paragraph 2, Guideline E:	AGAINST APPLICANT
Subparagraph 2.a:	Against Applicant
Paragraph 3, Guideline M:	AGAINST APPLICANT
Subparagraph 3.a:	Against Applicant
Subparagraph 3.b:	Against Applicant
Paragraph 4, Guideline J:	AGAINST APPLICANT
Subparagraph 4.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.

_____
PHILIP S. HOWE
Administrative Judge