DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 10-08390
	)	
	)	
Applicant for Security Clearance	)	

Appearances

For Government: David Hayes, Esquire, Department Counsel
For Applicant: Sheldon I. Cohen, Esquire

January 4, 2012

Decision

LYNCH, Noreen A., Administrative Judge:

After a review of the pleadings, exhibits, and testimony, I have questions and doubts as to Applicant's eligibility and suitability for a security clearance, as he has not mitigated the Government's security concerns. Applicant's eligibility for access to classified information is denied.

Applicant signed an Electronic Questionnaire for Investigations Processing (e-QIP) version of a security clearance application (SF-86) on October 21, 2009. The Defense Office of Hearings and Appeals (DOHA) issued Applicant a Statement of Reasons (SOR) on February 2, 2011, detailing security concerns under Guideline E (Personal Conduct), and Guideline M (Use of Information Technology Systems), that provided the basis for its preliminary decision to deny him a security clearance. 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 *Adjudicative Guidelines For Determining Eligibility for Access to Classified Information* (AG) implemented on September 1, 2006.

Applicant answered the SOR in writing on February 10, 2011, and requested a hearing before an administrative judge. I received the case assignment on July 25, 2011. DOHA issued a notice of hearing on October 14, 2011, and I convened the hearing as scheduled on November 17, 2011. The Government offered five exhibits marked as GE 1 through 5, which were admitted into evidence over objection. [1]Applicant testified, presented two witnesses, and submitted exhibits marked as AE A through I, which were admitted into evidence without objection. DOHA received the transcript of the hearing (Tr.) on November 29, 2011.

Findings of Fact

In his Answer to the SOR, Applicant admitted the factual allegations in ¶¶ 1.a, and 2.b of the SOR. He denied the other allegations. His admissions are incorporated herein as findings of fact. He also provided additional information to support his request for eligibility for a security clearance. After a complete and thorough review of the evidence of record, I make the following additional findings of fact.

Applicant is 60 years old. He attended college but did not obtain his undergraduate degree. Applicant has never married, and he has no children. He served on active duty in the military from 1969 until 1979. (AE A) Applicant served in the Navy reserves from July 1988 to May 1998. (AE B) He did not hold a security clearance in the military. (Tr. 71) Applicant is currently on administrative leave from his job. (GE 4)

He has served in the assurance security field since 1997. He held a top secret clearance in 2003, and had access to Sensitive Compartmented Information (SCI) in 2005. His security clearance was suspended in 2008 because he misused a government laptop to view pornographic web sites. (GE 5) He did not appeal the decision because he did not understand the process. (Tr. 125)

Applicant was assigned to various agencies from 2003 until 2009. His job responsibilities involved trouble shooting systems. (Tr. 96) He described his role as monitoring all activity on a computer system. He was also an accreditation engineer who made certain the systems adhered to a client's security policy. (Tr. 100) Applicant elaborated that he used an "intrusion detection system" for insider threat and outsider threat. (Tr. 105)

Applicant explained at the hearing that he detected pornography on an agency's computer system as part of his duties. (Tr. 105) He would then use tools to block it. If a malicious site was found, a report was written for the client. Thus, he explained that opening some sites that were designated as pornographic was a part of his job. (Tr. 107)

In 2004, Applicant underwent a series of polygraph tests during security processing. A letter addressed to Applicant from a Senior Adjudication Officer, states

[1]A pre-hearing telephone conference held on October 12, 2011, resulted in the denial of Applicant's Motion to bar the admission of GE 5. The Government did agree to strike the allegation in SOR Paragraph 2.b.

that as a result of Applicant's statements that he viewed adult pornography on government computers from 1996 until 2006, he was denied access to classified information on September 12, 2008. The letter further states that Applicant advised that he regularly viewed images of nude females between the ages of 11 and 16 on his home computer. (GE 2) Case notes from Applicant's file report that Applicant admitted he would routinely view pornography via the Internet on an average of two times per week at work as the rules were lax and there were no security policies. This was for the period October 1996 until October 2000. From October 2001 until February 2004, Applicant was deterred from pornographic activity due to "better computer and internal security measures, as well as cameras that monitored activities." (GE 5) The report concludes that Applicant stopped viewing pornography on a government computer. He knows it is wrong.

Finally, the case notes that are referenced above note that Applicant advised that he had about 50 images of underage pornography on his home computer. The children are hugging or kissing but not having sex according to Applicant. The same report notes that Applicant advised that until 2006, he visited teen chat rooms and frequently interacted sexually with other members. He also stated that in 2004, he was viewing approximately 20 images of naked 13 to 16 year olds per month. (GE 5)

At the hearing, Applicant testified that he has a number of computers in his home. His girlfriend testified that he has possibly four computers in his home. (Tr. 38) He views chat rooms on dating sites. He used it to interact with people his age. He acknowledged that some of the emails that are sent in a chat room contain nude pictures of females. (Tr. 113) He was adamant that he does not solicit emails with pictures of nude females. He was not sure if any of the emails had nude pictures of females under the age of 16, but he stated that he did not seek any of those sites. He denied entering any teen chat rooms.

In 2010, Applicant denied that he ever advised investigators that he viewed pornography except as part of his job duties. He denied that he regularly viewed images of nude females between the ages of 11 and 16. (GE 3) He maintained that he viewed pornography as part of his job. In essence, he denied the 2007 statements (admissions) that were attributed to him in the interviews and polygraphs that resulted in his 2008 suspension. At the hearing, Applicant again stated that the report/case notes from 2008 were falsifications and fabrications.

Applicant's hobbies include a motorcycle club. He spends his weekends with his friends in the club. His girlfriend usually accompanies him. He is active in volunteer activities for the community through the club. (AE H) Applicant tours schools and talks to students about motorcycle riders. He helps with veterans' projects. He is also an Assistant Director for a veterans' organization. (AE F)

Applicant submitted a packet of documents to include awards, letters of appreciation and commendations from 1984 until 2010. (AE B) They attest to the fact that Applicant went beyond expectations in every project. He brought credit to his team and to each contractor that he helped.

Applicant's significant other testified that she has known Applicant since July 2007. They see each other every weekend. (Tr. 29) She accompanies Applicant on his motorcycle rides with his club. She describes Applicant as a quiet gentleman. She also said he is a "nervous person." Applicant has met his friend's children. They have gone on vacation together. She testified that she believed the issue at hand was the result of a polygraph that "had gone bad." (Tr. 33) She elaborated that she knew Applicant was charged with viewing pornography at a work site. She has never seen Applicant at the computer viewing pornography nor has she known him to engage in chat rooms with teenagers. She testified that she would end the relationship if she believed he engaged in such behavior. Until the SOR was issued in July 2011, Applicant's friend had no knowledge of the allegations.

A friend from Applicant's motorcycle club testified that he has known him for about five years. He described Applicant's role in the club. The club does charity rides for local groups. There are a variety of activities that the club engages in, such as offering picnics or a holiday party. Applicant volunteers much of his time to the club. Applicant's friend was vague about his knowledge of the SOR allegations. He knew that the issue involved concerned looking at "something" more than he should have. (Tr. 60) He describes Applicant as a good person who is trustworthy. (Tr. 61)

Applicant presented a letter of recommendation from a colleague who holds a security clearance and has known Applicant for four years in a volunteer organization. He is aware of the allegations in the SOR. He attests to Applicant's integrity. He has never heard Applicant mention pornography or make a sexual joke. (AE I)

Policies

When evaluating an applicant's suitability for a security clearance, the administrative judge must consider the adjudicative guidelines. In addition to brief introductory explanations for each guideline, the adjudicative guidelines list potentially disqualifying conditions and mitigating conditions, which are used 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.

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. . . ." An applicant has the ultimate burden of persuasion for 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 an applicant may deliberately or inadvertently fail to protect or safeguard classified information. Such decisions entail a certain degree of legally permissible extrapolation as to potential, rather than actual, risk of compromise of classified information.

Section 7 of Executive Order 10865 provides that decisions shall be "in terms of the national interest and shall in no sense be a determination as to the loyalty of the applicant concerned." *See also* EO 12968, Section 3.1(b) (listing multiple prerequisites for access to classified or sensitive information).

Analysis

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 the disqualifying conditions that could raise security concerns. I have considered all the conditions, and especially the following: (e) unauthorized use of a government or other information technology system.

Applicant admitted that he viewed pornographic websites on a government computer while at work from approximately 1996 until 2006. Applicant's actions are a violation of the policies and regulations regarding the misuse of government-issued information technology equipment. The Government has established a *prima facie* case under Guideline M.

AG ¶ 41 provides 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.

Applicant's 2010 denial that he made the admissions in 2007 are not credible. He was denied a clearance based on the viewing of pornographic sites. The last viewing was in 2006. While this is five years ago, Applicant does not accept any responsibility for his actions. He has no insight into his behavior. His misconduct casts doubt on his current reliability. His conduct is not mitigated under AG ¶ 41(a).

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.

AG ¶ 16 describes the disqualifying conditions that could raise security concerns. I have considered all the conditions, and especially the following:

> (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;
>
> (c) credible adverse information in several adjudicative issue areas that is not sufficient for an adverse determination under any other single guideline, but which, when considered as a whole, 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;

(d) 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:

> (1) untrustworthy or unreliable behavior to include breach of client confidentiality, release of proprietary information, unauthorized release of sensitive corporate or other government protected information:
>
> (2) disruptive, violent, or other inappropriate behavior in the workplace;
>
> (3) a pattern of dishonesty or rule violations; and,
>
> (4) evidence of significant misuse of Government or other employer's time or resources;

(e) personal conduct, or 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, or (2) while in another country, engaging in any activity that is illegal in that country or that is legal in that country but illegal in the United States and may serve as a basis for exploitation or pressure by the foreign security or intelligence service or other group; and

(f) violation of a written or recorded commitment made by the individual to the employee as a condition of employment.

Applicant violated the work policy by viewing sexually explicit websites on his government-issued computer from 1996 until 2006. He also admitted to entering teen chat rooms and regularly viewed images of nude females between the ages of 11 and 16 on his home computer. As a result of this conduct, his clearance was suspended. He exercised poor judgment. The behavior is not appropriate. AG ¶¶ 16(c), 16(d), and 16(e)(1) apply.

AG ¶ 17 provides 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.

Applicant's conduct is not mitigated. He is not credible when he denies the admissions he made in 2007. It is not believable that the agency case notes are fabrications or falsifications. His serious misconduct casts doubt on his reliability and trustworthiness under these circumstances. He is subject to exploitation based on his behavior. He has not mitigated the personal conduct concerns.

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 relevant 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.

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. The decision to grant or deny a security clearance requires a careful weighing of all relevant factors, both favorable and unfavorable. In so doing, an administrative judge must review all the evidence of record, not a single item in isolation, to determine if a security concern is established and then whether it is mitigated. A determination of an applicant's eligibility for a security clearance should not be made as punishment for specific past conduct, but on a reasonable and careful evaluation of all the evidence of record to decide if a nexus exists between established facts and a legitimate security concern.

In reaching a conclusion, I considered the potentially disqualifying and mitigating conditions in light of all the facts and circumstances surrounding this case. Applicant has worked as a contractor for many years. He served in the military and retired honorably. He has received awards and recommendations. He is single, but in a significant relationship. He volunteers and does community work.

Applicant admitted during a security process investigation that he viewed pornographic websites on government computers while at work from about 1996 until 2006. However, his explanation that it was part of his job duties is not credible. He admitted during a 2007 polygraph to the allegations in the SOR. His denials in 2010 and at the hearing are not persuasive. He has not shown candor or accepted responsibility for his behavior. This is serious and spans a ten-year period. He has no insight into his behavior. He does not accept responsibility for the behavior.

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 has not mitigated the security concerns arising from his misuse of information technoloy under Guideline M and his personal conduct under Guideline E.

Formal Findings

Formal findings for or against Applicant on the allegations set forth in the SOR, as required by section E3.1.25 of Enclosure 3 of the Directive, are:

Paragraph 1, Guideline M:	AGAINST APPLICANT
Subparagraph 1.a:	Against Applicant
Paragraph 2, Guideline E:	AGAINST APPLICANT

Subparagraph 2.a:	Against Applicant
Subparagraph 2.b:	WITHDRAWN
Subparagraph 2.c:	Against Applicant
Subparagraph 2.d:	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.

Noreen A. Lynch
Administrative Judge