



**DEPARTMENT OF DEFENSE  
DEFENSE OFFICE OF HEARINGS AND APPEALS**



In the matter of:	)	
	)	
	)	
	)	ISCR Case No. 07-13466
	)	
	)	
Applicant for Security Clearance	)	

**Appearances**

For Government: John Bayard Glendon, Esquire, Department Counsel  
For Applicant: *Pro Se*

November 25, 2008

\_\_\_\_\_

**Decision**

\_\_\_\_\_

ANTHONY, Joan Caton, Administrative Judge:

After a thorough review of the case file, pleadings, testimony, and exhibits, I conclude that Applicant failed to rebut or mitigate the Government's security concerns under Guideline D, Sexual Behavior, Guideline E, Personal Conduct, and Guideline M, Use of Technology Systems. His eligibility for a security clearance is denied.

Applicant submitted a Security Clearance Application (SF-86) on February 27, 2007. On June 19, 2008, the Defense Office of Hearings and Appeals (DOHA) issued Applicant a Statement of Reasons (SOR) detailing the security concerns under Guideline D, Sexual Behavior, Guideline E, Personal Conduct, and Guideline M, Use of Technology Systems. 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.

On August 11, 2008, Applicant answered the SOR in writing and, at a later time, after reviewing the investigative record compiled in his case, elected to have a hearing before an administrative judge. The case was assigned to me on October 2, 2008. I convened a hearing on October 29, 2008, to consider whether it is clearly consistent with the national interest to grant or continue a security clearance for Applicant. The Government called no witnesses and introduced two exhibits, which were marked Ex. 1 and Ex. 2 and admitted to the record without objection. Applicant testified on his own behalf, called one witness, and introduced one exhibit, which was marked Ex. A. Applicant's Ex. A was admitted to the record without objection.

DOHA received the transcript (Tr.) of the hearing on November 6, 2008.

### **Findings of Fact**

The SOR contains eight allegations of disqualifying conduct under AG D, Sexual Behavior (SOR ¶¶ 1.a. and 1.h.), two allegations of disqualifying conduct under AG E, Personal Conduct (SOR ¶¶ 2.a. and 2.b.), and one allegation under AG M, Use of Information Technology Systems (SOR ¶ 3.a.). In his Answer to the SOR, Applicant admitted three allegations under AG D and one allegation under AG E. He denied six allegations under AG D, one allegation under AG E, and one allegation under AG M. Applicant's admissions are admitted herein as findings of fact.

Applicant is 45 years old and employed by a government contractor. He graduated from a military college with a bachelor's degree in civil engineering, and he served on active duty in the military from 1985 to 1992. From 1992 to 1999, Applicant served as an inactive military reservist at the rank of captain. He was first granted a security clearance in 1986. In 1988, he was granted eligibility for access to Sensitive Compartmented Information (SCI). Since returning to civilian life in 1992, Applicant has been employed by six government contractors.<sup>1</sup> (Ex. 1; Ex. 2; Tr. 27-29, 33-35.)

Applicant was married in 1985. He and his wife are the parents of four daughters and three sons. Applicant's oldest child is 21 years old; his youngest child is four years old. Applicant's wife filed for divorce in July 2008. (Ex. 1; Tr. 63-64, 68.)

Since adolescence, Applicant has battled a strong and repetitive desire to access and view pornography. While he denies he is addicted, Applicant has regularly accessed pornography at home and in his workplaces for over 20 years. He considers viewing pornography to be sinful and morally wrong. He has stated: "I realize I will always be tempted to view pornography as it has been an ongoing battle my entire life." (Tr. 65-66; Ex. 2 at 14.)

---

<sup>1</sup> Applicant was employed by federal contractor X from October 2001 to August 2004. He returned to work for federal contractor X in July 2007. Federal contractor X is the sponsor of his current request for a security clearance.

Since becoming committed to his faith in 1986, he has sought support and counsel from fellow members of his church and from his pastors in addressing his attraction to and use of pornography. In an affidavit he signed in January 2008, he stated he had never gone outside of his faith community for help with his pornography problem. He told an authorized investigator in January 2008 that he would be open to seeking professional psychological counseling for his problem with the repetitive use of pornography. As of the date of his ISCR hearing, he had not taken any action to seek outside professional help. While at his hearing he repeated his openness to seeking treatment, he also stated that, on his own, he had successfully changed the behavior which led him to seek pornography. (Ex. 2; Tr. 45-52.)

Applicant searched for and viewed pornographic images on his official work computers when employed by four separate government contractors during the periods from 1992 to 1996, 1996 to 1999, 2001 to 2004, and 2005 to 2007. Applicant knew his employers had policies prohibiting the use of office computers to access pornography. He also knew that by using his workplace computers to access and view pornography, he was violating his employers' policies and his agreements to abide by those policies. He preferred to access and view pornography at work because he feared discovery by his wife or children if he used pornography at home. When he elected to access and view pornographic images and movies in the workplace, he took steps to hide his behavior from his employers. If he had a private office, he stayed late and viewed pornography after regular work hours. He also stated that after viewing pornography, he involved himself with masturbation in his office or in a workplace bathroom. Applicant did not tell his employers about his use of pornography in the workplace because he feared losing his job and other possible adverse consequences. (Ex. 2 at 5, 8; Tr. 54-58.)

In August 2004, Applicant accepted a position with a government contractor. The position required that he hold a security clearance and be granted eligibility for access to SCI. As a part of his background investigation, Applicant underwent a polygraph examination conducted by another federal agency. From the facts that Applicant provided on the polygraph, the other agency denied his request for a security clearance and access to SCI because it concluded that his use of pornography included searching for and viewing pornographic images of underage females. Applicant denied actively seeking or using child pornography. He stated he sought and used only adult heterosexual pornography. He acknowledged that he had no way of knowing or verifying the ages of the females whose pornographic images he had viewed over the course of many years. He also stated that he was attracted to and considered pornography involving teen-aged girls to be legal pornography. (Ex. 2 at 6; Tr. 61-63.)

In May 2005, after being denied the security status requested by the employer, Applicant moved to another job with a different government contractor. He stated he informed his supervisor at his new job that he had been denied a security clearance because he had misused his former employers' information technology systems. He also stated he told his new employer's security officer that he had lost his clearance because he had viewed pornography. During this employment, Applicant accessed and

viewed pornography on his employer's information technology systems. Applicant was laid off by this employer in May 2007. He stated that he had last accessed and viewed pornography on an employer's workplace computer in February 2007. (Ex. 2 at 1-2, 4-8; Tr. 20, 52-59.)

Sometime after being laid off, Applicant accepted a position with a government contractor he had worked for previously. In January 2008, after providing an affidavit to an authorized investigator from the U.S. Office of Personnel Management (OPM), Applicant asked his employer's security officer to monitor his compliance with the company's computer security requirements. The employer's manager for security and safety monitored Applicant's compliance from January 10, 2008 to October 22, 2008 and found Applicant to be in compliance with company security requirements. Applicant denies ever using his employers' classified computers or classified networks to access and view pornography. (Ex. 2 at 8; Ex. A.)

Applicant's wife and his three oldest children know of his personal battles with pornography. Applicant's wife also knows that he used his employers' information technology systems to access and view pornography and that these actions have caused him to lose access to classified information. Applicant has a personal computer in his home which he uses to access and view pornography. In 2004, Applicant had a pornography monitoring program installed on his personal computer. The monitoring system was designed to block pornography so that Applicant could not access or view it. The monitoring program remained on Applicant's personal computer for approximately 1½ years. During that time, Applicant figured out how to bypass the monitoring system and access and view pornography without anyone knowing. (Ex. 2 at 9, 13-14; Tr. 69-70.)

In the summer of 2007, Applicant again had a pornography monitoring program installed on his personal computer. This program was designed to monitor Applicant's internet browsing and report the results to two people selected by him. Applicant used this program for several months. He then removed it from his computer because he said it caused his computer to "run slowly and block some functions I needed to perform on it." In January 2008, after his interview with an authorized investigator, he reinstalled the program again on his computer. (Ex. 2 at 13, 17.)

In the last six months Applicant has viewed pornographic images about three times. In addition to computer searches for pornography, he also rents pay-per-view pornographic movies monthly. In an attempt to control his viewing of pornographic movies, Applicant has tasked his 21-year-old son with holding the PIN number authorizing access to pay-for-view pornography. (Ex. 2 at 13; Tr. 65-68.)

Applicant and his wife are separated, and his wife has filed for divorce. Applicant accuses his wife of an extra-marital same-sex relationship. He hopes to reconcile with his wife. In the event the couple does not reconcile and Applicant's wife is granted a divorce, Applicant intends to sue for custody of their minor children. (Tr. 74-78.)

Applicant's pastor, who has known him for over 15 years, testified about his efforts and those of other church members to help Applicant overcome his attraction to and compulsive use of pornography. (Tr. 84-99.)

### **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, the administrative judge applies these guidelines in conjunction with the factors listed in the adjudicative process. The administrative judge's over-arching 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 D, Sexual Behavior**

AG ¶12 identifies the government’s concern with Guideline D, in pertinent part, as follows:

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

While he denies an addiction to pornography, Applicant, who is now 45 years old and the father of seven children, acknowledges that, since adolescence, he has battled a compulsive desire to access and view pornographic material. Because the record does not contain a medical diagnosis of sexual addiction, I conclude SOR ¶ 1.b. for Applicant. Applicant made an affirmative choice over a period of twenty years to seek help from his church community in controlling his desire to view pornography. That the help failed to permanently change or mitigate his behavior does not negate his efforts. I also conclude SOR ¶ 1.c. for Applicant.

For at least four protracted periods of time, between 1992 and 2007, his strong and repetitive desire to view pornography caused him to use his employers’ information technology systems to access and view pornography. Applicant vigorously denied that he sought or used child pornography, but did not deny he had accessed and viewed pornography involving teen-aged girls because he considered pornography involving teen-aged girls to be legal pornography and found it impossible to determine with accuracy whether the individuals on the pornographic images he viewed were adults. Applicant’s behavior in viewing pornographic images in the workplace as a government contractor reflected lack of discretion and judgment and made him vulnerable to the possibility of coercion, exploitation and duress. I conclude that his sexual behavior raises security concerns under AG ¶¶ 13(b), 13(c), and 13(d).<sup>2</sup>

An applicant might be able to mitigate Guideline D security concerns. If the sexual “behavior occurred prior to or during adolescence and there is no evidence of subsequent conduct of a similar nature,” then AG ¶ 14 (a) might apply. If “the sexual

---

<sup>2</sup> AG ¶ 13(b) reads: “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.” AG ¶ 13(c) reads: “sexual behavior that causes an individual to be vulnerable to coercion, exploitation, or duress.” AG ¶ 13(d) reads: “sexual behavior of a public nature and/or that reflects lack of discretion or judgment.”

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," then AG ¶ 14(b) might apply. If "the behavior no longer serves as a basis for coercion, exploitation, or duress," the AG ¶ 14(c) might apply. Finally, if "the sexual behavior is strictly private, consensual, and discreet," then AG ¶14 (d) might apply. Applicant was an adult when he carried out the sexual behavior that raises security concerns. He denied his behavior could be defined as a sexual addiction, and he did not seek an evaluation of his sexual behavior from a qualified professional counselor. His sexual behavior was indiscreet and reflected poor judgment. It was repetitive and involved taking high risks that made him vulnerable to coercion, exploitation, or duress. I conclude that none of the Guideline D mitigating conditions apply to the facts of Applicant's case.

### **Guideline E, Personal Conduct**

Under the Personal Conduct guideline "[c]onduct 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 ¶ 15

Applicant's high risk sexual behavior was in contravention of the security policies of his government contractor employers. He purposefully concealed his access and use of pornography in the workplace from his employers because he knew he might lose his job if his behavior was discovered. He also betrayed the trust of his family, church community, and those who sought to counsel and support him in overcoming his compulsive use of pornography when he disabled computer monitoring controls intended to block his access to pornography. I have carefully considered all of the Personal Conduct Disqualifying conditions. I have especially considered AG ¶ 16(e), which reads as follows: "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 . . . ."

During his military and civilian careers, Applicant was awarded a security clearance. He then engaged in high risk sexual behavior that he kept secret and did not report to his security officers, making him vulnerable to exploitation, manipulation, or duress. His compulsive use of pornography in the workplace, if known, would have affected his personal, professional, and community standing because it raised issues of trustworthiness and reliability. Accordingly, I conclude that AG ¶16(e)(1) is raised by the facts of Appellant's case.

Applicant's disqualifying personal conduct might be mitigated if he "made prompt, good-faith efforts to correct the omission, concealment, or falsification before being confronted with the facts." AG ¶ 17(a) Additionally, Applicant's disqualifying conduct

might be mitigated if he “has taken positive steps to reduce or eliminate vulnerability to exploitation, manipulation, or duress.” AG ¶ 17(e)

Applicant did not make prompt good faith efforts to correct his concealment. He has not addressed whether he has a sexual addiction that would lead future high-risk sexual behavior and a similar pattern of concealment. I conclude that neither AG ¶ 17(a) nor AG ¶ 17(e) applies to the facts of Appellant’s case.

### **Guideline M, Use of Information Technology Systems**

AG ¶ 39 identifies the Government’s concern under the Use of Information Technology Systems adjudicative guideline:

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.

For more than 20 years, Applicant used his employers’ computers to access and view pornographic materials. His actions contravened his employers’ policies as government contractors and raised security concerns about Applicant’s willingness or ability to put the Government’s interest in protecting classified information ahead of his own desires. Applicant’s behavior raises a security concern under AG ¶ 40(e), which reads: “unauthorized use of a government or other information technology system.”

Three possible mitigating conditions could apply to security concerns arising under AG ¶ 40. If “so much time has elapsed 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,” then AG ¶ 41(a) might apply. If “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,” then AG ¶ 41(b) might apply. Finally, if “the conduct was unintentional and inadvertent and was followed by a prompt, good-faith effort to correct the situation and by notification of supervisor,” then AG ¶ 41(c) is applicable.

Applicant’s misuse of his employers’ information technology systems was neither minor nor justified in the interest of organizational efficiency and effectiveness. Applicant’s last admitted misuse of an employer’s information technology system to access pornography occurred in February 2007. When viewed in light of Applicant’s 20 years of secretive and deliberate misuse, insufficient time has elapsed to conclude that Applicant is now reliable and trustworthy and will not likely misuse a government



employer's information technology system again to access pornography. Accordingly, I conclude that none of the mitigating conditions identified under AG ¶ 41 apply to the fact of Applicant's case.

### **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) 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.

I considered the potentially disqualifying and mitigating conditions in light of all the facts and circumstances surrounding this case. Over a period encompassing 1992 to 1996, 1996 to 1999, 2001 to 2004, and 2005 to 2007, Applicant violated the security policies of four different government contractors by accessing and viewing pornography on information technology systems owned by his employers and used for their work as government contractors. He kept his actions secret from his employers. He deceived his family and those in his church community who sought to help him control his compulsive desire to access and view pornography. While he asserted he would seek professional counseling for his compulsive behavior, he failed to do so and averred he had successfully resolved the problem on his own. He failed to mitigate serious concerns about his credibility, reliability, trustworthiness, and ability to put the government's interests before his own in the protection of classified information. AG ¶ 2(a)(7).

Overall, the record evidence leaves me with questions and doubts as to Applicant's eligibility and suitability for a security clearance. For these reasons, I conclude Applicant failed to mitigate the security concerns arising from his sexual behavior, personal conduct, and use of information technology systems.

## 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:	For Applicant
Subparagraph 1.c:	For Applicant
Subparagraph 1.d:	Against Applicant
Subparagraph 1.e:	Against Applicant
Subparagraph 1.f:	Against Applicant
Subparagraph 1.g:	Against Applicant
Subparagraph 1.h:	Against Applicant
Paragraph 2, Guideline E:	AGAINST APPLICANT
Subparagraph 2.a:	Against Applicant
Subparagraph 2.b:	Against Applicant
Paragraph 3, Guideline M:	AGAINST APPLICANT
Subparagraph 3.a:	Against Applicant

## Conclusion

In light of all of the circumstances presented by the record in this case, it is not clearly consistent with national security to grant Applicant eligibility for a security clearance. Eligibility for access to classified information is denied.

---

Joan Caton Anthony  
Administrative Judge