DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
----------	)	ISCR Case No. 07-04193
SSN: ----------	)	
	)	
Applicant for Security Clearance	)	

Appearances

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

March 19, 2008

Decision

TESTAN, Joseph, Administrative Judge:

On September 25, 2007, the Defense Office of Hearings and Appeals (DOHA) issued a Statement of Reasons (SOR) to applicant detailing the security concerns under Guidelines E, J and M. The action was taken under Executive Order 10865, *Safeguarding Classified Information Within Industry* (February 20, 1960), as amended; Department of Defense Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (January 2, 1992), as amended (Directive); and the revised adjudicative guidelines (AG) promulgated by the President on December 29, 2005, and effective within the Department of Defense for SORs issued after September 1, 2006.

Applicant answered the SOR in writing on October 17, 2007, and requested an Administrative Determination by an Administrative Judge (AJ). Department Counsel issued a File of Relevant Material (FORM) on December 7, 2007. Applicant filed an undated response to the FORM. Based upon a review of the case file, pleadings, and exhibits, eligibility for access to classified information is denied.

Findings of Fact

Applicant is a 52 year old employee of a defense contractor.

Applicant was fired from his government contractor employer (Employer A) in 2000 for continued violations of the company's internet policy; namely, viewing sexually explicit websites on his company computer. He had previously been counseled about viewing pornographic web sites on his company computer during duty hours.

While working for Employer B in 2001, applicant accessed and viewed pornographic websites, and downloaded material from said websites, during work hours. His employer never found out about this activity, which was prohibited by company policy.

In May 2002, applicant was counseled by his employer (Employer C) about his need to work on government contracts instead of accessing pornographic websites on the company computer. He received this counseling after it was determined he had downloaded approximately 145 pornographic videos onto his computer. After this counseling, his computer activities were monitored by his employer without his knowledge. In August 2002, he was observed accessing pornographic websites and was fired.

Applicant falsified material facts on an Electronic Questionnaire for National Security Positions (EQNSP) he executed in March 2006 when he lied about the reasons he was fired by Employers A and C. He lied because he was afraid that if he revealed he was fired for viewing pornography on company computers, it might adversely affect his security clearance.

Applicant lied about the reason he was fired from Employer C during an interview with an OPM investigator in August 2006. He lied because he was afraid that if he told the truth, it could adversely affect his security clearance.

In a signed, sworn statement he gave to a Special Agent of the DSS in September 2007, applicant stated that he could not state "with 100% certainty" that he would not access pornographic websites at his place of employment.

In response to the FORM, applicant stated that following his termination from Employer C, he promised his wife that he "would not risk losing employment by improperly using company assets to access pornography at any future work place." He further stated, "This promise is the main reason I have been successful in only using IT systems as allowed by the rules of the organization in which I worked since August 2002." He further stated that he has recently started counseling on his "pornography problem."

Policies

The President has "the authority to . . . control access to information bearing on national security and to determine whether an individual is sufficiently trustworthy to

occupy a position that will give that person access to such information." *(Department of the Navy v. Egan,* 484 U.S. 518,527 (1988).) In Executive Order 10865, *Safeguarding Classified Information Within Industry* (February 20, 1960), the President set out guidelines and procedures for safeguarding classified information within the executive branch. The President authorized the Secretary of Defense or his designee to grant applicants eligibility for access to classified information "only upon a finding that it is clearly consistent with the national interest to do so." (Exec. Ord. 10865, Section 2.)

To be eligible for a security clearance, an applicant must meet the security guidelines contained in the Directive. Enclosure 2 of the Directive sets forth personnel security guidelines, as well as the disqualifying conditions and mitigating conditions under each guideline.

Initially, the Government must present evidence to establish controverted facts in the SOR that disqualify or may disqualify the applicant from being eligible for access to classified information. (Directive, Paragraph E3.1.14.) Thereafter, the applicant is responsible for presenting evidence to rebut, explain, extenuate, or mitigate the facts. (Directive, Paragraph 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).) "Any doubt as to whether access to classified information is clearly consistent with national security will be resolved in favor of the national security." (Directive, Paragraph E2.2.2.)

A person granted access to classified information enters into a special relationship with the government. The government must be able to repose a high degree of trust and confidence in those individuals to whom it grants access to classified information. The decision to deny an individual a security clearance is not a determination as to the loyalty of the applicant. (Exec. Ord. 10865, Section 7.) It is merely an indication that the applicant has not met the strict guidelines the President has established for issuing a clearance.

Analysis

Guideline E, Personal Conduct

The security concern relating to the guideline for Personal Conduct is set forth in Paragraph 15 of the AG, and is as follows:

> 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.

Paragraph16 describes conditions that could raise a security concern and may be disqualifying. Under Paragraph 16.a., the "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," may be disqualifying. Under Paragraph 16.b, "deliberately providing false or misleading information concerning relevant facts to an employer, investigator, security official, competent medical authority, or other official government representative" may be disqualifying. These disqualifying conditions are applicable because applicant intentionally provided false, material information on an EQNSP and to an OPM investigator.

Paragraph 17 sets forth conditions that could mitigate security concerns. I considered each of them and conclude none apply.

Guideline J, Criminal Conduct

The security concern for criminal conduct is set forth in Paragraph 30 of the AG, and is as follows:

> 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.

Paragraph 31 describes conditions that could raise a security concern and may be disqualifying: Under Paragraph 31.a., "a single serious crime or multiple lesser offenses" may be disqualifying. And, under Paragraph 31.c., an "allegation or admission of criminal conduct, regardless of whether the person was formally charged, formally prosecuted or convicted," may be disqualifying. Applicant's multiple falsifications were felonies under 18 U.S.C. 1001. Accordingly, these two disqualifying conditions are applicable.

Paragraph 32 of the AG sets forth conditions that could mitigate security concerns. I have considered each of them and conclude none apply.

Guideline M, Use of Information Technology Systems

The security concern for use of information technology systems is set forth in Paragraph 39 of the AG, and is as follows:

> 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.

Paragraph 40 describes conditions that could raise a security concern and may be disqualifying. Under Paragraph 40.e., "unauthorized use of a government or other information technology system" may be disqualifying. Given applicant's use of his

employers' computers to access pornography in violation of their IT rules and regulations, this disqualifying condition applies.

Paragraph 41 of the AG sets forth the conditions that could mitigate security concerns. None are applicable.

"Whole Person" Analysis

Under the whole person concept, the AJ must evaluate an applicant's security eligibility by considering the totality of the applicant's conduct and all the circumstances. An AJ should consider the nine adjudicative process factors listed at AG Paragraph 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 Paragraph 2c, the ultimate determination of whether to grant a security clearance must be an overall common sense 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 is a mature man who has a history of ignoring his employers' IT policies by accessing, viewing, and downloading pornography onto his employers' computers. This conduct resulted in applicant being terminated from two employers, information applicant attempted to conceal from the Government. His conduct was intentional, serious, and frequent. Applicant has taken a big step in the right direction by seeking counseling for what he describes as a pornography addiction, but as he has admitted, he is not 100% certain he will be able to comply with the IT policies of his employers in the future. Under the circumstances, applicant failed to mitigate the security concerns arising from Guidelines E , J and M.

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. through 1.f:	Against Applicant
Paragraph 2, Guideline M:	AGAINST APPLICANT
Paragraph 3, Guideline J:	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.

JOSEPH TESTAN
Administrative Judge