DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
----------.	)	
SSN: ----------	)	ISCR Case No. 06-22281
	)	
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Jennifer Goldstein, Esquire, Department Counsel
For Applicant: Pro Se

October 31, 2008

_____

Decision

_____

LYNCH, Noreen, Administrative Judge:

On November 1, 2005, Applicant submitted an Electronic Questionnaire for Investigations Processing (e-QIP) to request a security clearance for his employment with a defense contractor. After reviewing the results of the ensuing background investigation, adjudicators for the Defense Office of Hearings and Appeals (DOHA) were unable to make a preliminary affirmative finding[1] that it is clearly consistent with the national interest to grant Applicant's request. On July 31, 2008, DOHA issued to Applicant a Statement of Reasons (SOR) alleging facts which raise security concerns addressed in the Revised Adjudicative Guidelines (AG)[2] under Guideline M (misuse of information technology) and Guideline E (personal conduct).

[1] Required by Executive Order 10865, as amended, and by DoD Directive 5220.6 (Directive), as amended.

[2] Adjudication of this case is controlled by the Revised Adjudicative Guidelines, approved by the President on December 29, 2005,which were implemented by the Department of Defense on September 1, 2006. Pending official revision of the Directive, the Revised Adjudicative Guidelines supercede the guidelines listed in Enclosure 2 to the Directive, and they apply to all adjudications or trustworthiness determinations in which an SOR was issued on or after September 1, 2006.

Applicant timely responded to the SOR, and admitted all of the allegations in the SOR. He elected to have his case decided on the record in lieu of a hearing. Department Counsel submitted the Government's written case on August 29, 2008.[3] Applicant received a complete file of relevant material (FORM) on September 12, 2008, and was provided an opportunity to file objections and submit material to refute, extenuate, or mitigate the Government's case. Applicant submitted additional information on September 22, 2008. The case was assigned to me on October 21, 2008. Based upon a review of the case file, pleadings, exhibits, and testimony, Applicant's request for a security clearance is denied.

Findings of Fact

Under Guideline M, the government alleged in SOR ¶ 1.a that Applicant misused government resources while employed from 2002 to 2004 during work and non-work hours by using his computer to access inappropriate web sites, to include those of a pornographic nature. In SOR ¶ 1.b, the government alleged Applicant installed software that could erase system memory on his computer from 2002 to 2004. In SOR ¶ 1.c., the government alleged Applicant sent a joke from a pornographic web site in 2004 to a co-worker.

Under Guideline E, the government alleged in SOR ¶ 2.a the same information alleged in SOR ¶ 1.a. The government also alleged falsification in SOR ¶¶ 2.b. through d. After a thorough review of the pleadings, transcript, and exhibits, I make the following findings of fact.

Applicant is 54 years old. Since April 2004, he has worked as a systems analyst for a defense contractor. In 2003, he graduated from college with a B.S. degree. Applicant served in the U.S. Army from 1996 until 2002, and held a security clearance. He also held a clearance during his civilian employment until his resignation in 2004 (Item 4).

Applicant worked as a civilian employee from 2002 until 2004. During that time, he admits sending inappropriate email to a coworker. The email contained a photograph of a pornographic nature. An investigation revealed that he also installed software that he could use to erase system memory. Applicant visited many sites on the internet during work and non-work hours on his government computer that were considered pornographic. He spent approximately two hours per day, on average, searching the internet for these sites (Item 9). The record reveals that he was counseled at some point in time about the inappropriate use (Item 11).

On February 17, 2004, a complaint was filed against Applicant. An investigation followed and Applicant was sent back to work. However, his computer was taken. Applicant resigned his position on April 4, 2004 (Item10).

[3]The Government submitted eleven items to support its case.

Applicant completed a security clearance application in November 2005. He answered Section 22: Your Employment Record. His response to the question concerning the reasons for resigning a job under unfavorable circumstances was "no." Applicant explained that he did resign but he had reasons in addition to 'unfavorable circumstances.' He claimed he was subject to weekly interrogations and saw no punishment in sight. He began to feel harassed (Applicant's answer to FORM, undated).

A Department of Defense investigator interviewed Applicant on August 9, 2006 (Item 5). He reported that he used the computer once to visit a pornographic web site. In his answer, he admitted that he falsified material facts by not disclosing that he had accessed the pornographic sites on many occasions. He did not provide any information or explanation that would permit mitigation.

Applicant teaches classes to graduates and undergraduates on post on the "dos and don'ts' of security issues. He wants to pass on the lesson that he has learned from his mistake. He is also taking post graduate courses in information security. He is sorry for his mistakes.

Policies

Each security clearance decision must be a fair, impartial, and commonsense determination based on examination of all available relevant and material information, and consideration of the pertinent criteria and adjudication policy in the Revised Adjudicative Guidelines (AG).[4] Decisions must also reflect consideration of the factors listed in ¶ 2(a) of the new guidelines.[5] The presence or absence of a disqualifying or mitigating conditions is not determinative of a conclusion for or against an applicant. However, specific applicable guidelines should be followed whenever a case can be measured against them as they represent policy guidance governing the grant or denial of access to classified information. In this case, the pleadings and the information presented by the parties require consideration of the security concerns and adjudicative factors addressed under Guideline M (misuse of information technology systems), at AG ¶ 39, and Guideline E (personal conduct) at AG ¶ 15.

A security clearance decision is intended to resolve whether it is clearly consistent with the national interest[6] for an applicant to either receive or continue to have access to classified information. The government bears the initial burden of producing admissible information on which it based the preliminary decision to deny or

[4] Directive. 6.3.

[5] Commonly referred to as the "whole person" concept, these factor are: (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.

[6] *See Department of the Navy v. Egan*, 484 U.S. 518 (1988).

revoke a security clearance for an applicant. Additionally, the government must be able to prove controverted facts alleged in the SOR. If the government meets its burden, it then falls to the applicant to refute, extenuate or mitigate the government's case. Because no one has a "right" to a security clearance, an applicant bears a heavy burden of persuasion.[7] A person who has access to classified information enters into a fiduciary relationship with the government based on trust and confidence. The government, therefore, has a compelling interest in ensuring each applicant possesses the requisite judgement, reliability and trustworthiness of one who will protect the national interests. The "clearly consistent with the national interest" standard compels resolution of any reasonable doubt about an applicant's suitability for access in favor of the government.[8]

Analysis

Misuse of Information Technology Systems.

Under Guideline M, "[n]oncompliance 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 ¶ 39). The government presented sufficient information to support the allegations in SOR ¶¶ 1.a, 1.b, and 1.c. Applicant admitted using his computer at work to access inappropriate web sites, to include those of a pornographic nature. The information presented requires consideration of the disqualifying condition listed at AG ¶ 40(e) (*unauthorized use of a government or other information technology system*).

The record does support consideration of Guideline M mitigating conditions listed in AG ¶ 41. This conduct last occurred in 2004. Since then, Applicant has taught graduate and undergraduate classes on security for several years to share his knowledge and impart the lessons that he has learned from this experience. He is also taking classes in information security for his benefit. He acknowledges his inappropriate actions and admits it was wrong. Applicant has demonstrated how his actions do not reflect adversely on his current "reliability, trustworthiness, or good judgment." (AG ¶ 41(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*).

[7] *See Egan,* 484 U.S. at 528, 531.

[8] *See Egan;* Revised Adjudicative Guidelines, ¶ 2(b).

Personal Conduct.

The security concern about Applicant's personal conduct, as expressed in the AG ¶ 15, is that "[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."

As to SOR ¶ 2.b, available information requires consideration of the disqualifying conditions listed in AG ¶ 16(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 admitted that he initially denied any inappropriate computer activity during his interview in 2004 and in an August 9, 2006 interview with an investigator for DoD. On his November 1, 2005 security clearance application, he answered "no" to Section 22: Your Employment Record and failed to disclose that he resigned from employment in 2004 following his investigation about the computer misuse. For these reasons, the record does not warrant application of any of the mitigating conditions listed under AG ¶ 17.

Whole Person Concept.

I have evaluated the facts presented in this record and have applied the appropriate adjudicative factors, pro and con, under Guidelines M and E. I have also reviewed the record before me in the context of the whole person factors listed in ¶ AG 2(a).[9] Applicant is a mature adult who held a security clearance for many years. Since the 2004 resignation, Applicant has taught classes in security information and tried to impart the lesson that he learned from his inappropriate use of his government computer. He acknowledges his mistake and is sorry for the incident. The positive information about Applicant is sufficient to overcome the adverse information about his conduct at his previous job under Guideline M. However, the falsification of information during his investigations and on his November 2005 security application raise serious doubts about his reliability and trustworthiness. Applicant's recent conduct does not mitigate the security concerns under the personal conduct guideline. Because protection of the national interest is paramount in these determinations, such doubts must be resolved in favor of the national interest.[10]

Formal Findings

Formal findings 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: FOR APPLICANT

[9] *See* footnote 5, *supra.*

[10] *See* footnote 8, *supra.*

Subparagraph 1.a:	For Applicant
Subparagraph 1.b:	For Applicant
Subparagraph 1.c:	For Applicant
Paragraph 2, Guideline E:	AGAINST APPLICANT
Subparagraph 2.a:	For Applicant
Subparagraph 2.b:	Against Applicant
Subparagraph 2.c:	Against Applicant
Subparagraph 2.d:	Against Applicant

Conclusion

In light of all of the foregoing, 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