DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
----------	)	
SSN: ----------	)	ISCR Case No. 07-05146
	)	
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Emilio Jaksetic, Esquire, Department Counsel
For Applicant: William F. Savarino, Esquire

April 15, 2008

Decision

LYNCH, Noreen, Administrative Judge:

On October 29, 2007, the Defense Office of Hearings and Appeals (DOHA) issued to Applicant a Statement of Reasons (SOR) detailing the basis for its preliminary decision to deny his application for a security clearance. The SOR cited security concerns under Guidelines M (misuse of information technology) and Guideline E (personal 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 timely responded to the SOR, admitting all of the allegations therein, and requested a hearing. The case was assigned to me on February 27, 2008, and I scheduled a hearing to be held on April 1, 2008. The parties appeared as scheduled. The government presented seven exhibits (GE. 1 - 7). Applicant testified, offered 44 exhibits (AE. A - OO), and presented six witnesses. DOHA received the transcript (Tr.)

on April 10, 2008. Based upon a review of the case file, pleadings, exhibits, and testimony, Applicant's request for a security clearance is granted.

Findings of Fact

Under Guideline M, the government alleged in SOR ¶ 1.a that Applicant was counseled in May 2004 for viewing, downloading and/or sending pornography on his government computer and/or government networks system. In SOR ¶ 1.b, the government alleged Applicant was investigated by the Office of the Inspector General on December 22, 2004, concerning continued misuse of government equipment and communications systems; that the investigation revealed that Applicant had viewed, downloaded and/or sent pornography depicting nude women and adults engaged in sexually explicit acts on his government computer and/or government networks system; that Applicant received a formal letter of reprimand with a two-year probation condition that any future infractions will be termination for cause; and that an adverse report was filed on June 6, 2005.

Under Guideline E, the government alleged in SOR ¶ 2.a the same information alleged in SOR ¶ 1.a. Applicant's admissions are entered as facts. After a thorough review of the record, I make the following additional findings of fact.

Applicant is 51 years old. Since November 2000, he has worked as a systems analyst for a defense contractor. He has held a top secret clearance in the military and in his civilian career. He served in the U.S. Marine Corps (USMC) from 1977 until December 2000 (Tr. 129). He is married with no children.

Applicant works as part of a team to support the Navy-Marine Corps Intranet (NMCI). He works with other government employees and contractors. He is the contract technical representative who provides technical support to the Director, NMCI. He is also the assistant security officer. His clearance affords him access to government facilities and national security information (GE 1).

In 2003, Applicant received joke emails on his government computer from high ranking officials and service personnel that contained inappropriate material. The emails included photographs and videos of nude women. He forwarded these emails to a group of friends and other Marines in his address book. He admitted that he viewed and downloaded the pornographic images (depicting nude women and adults engaged in sexually explicit acts) in violation of policy, contract and regulations. In May 2004, Applicant was counseled by his employer to discontinue the use (GE 2). However, he continued the practice when he received more emails in the following months (Tr. 135). When Applicant spoke to one of his supervisors about the emails in 2004, his supervisor joked and told him not to do it again (Tr 137).

In March 2005, Applicant received a phone call from an investigator in the Inspector Generals Office (IG). The Applicant answered questions concerning the inappropriate email use on the computer at work. After the telephone conversation, Applicant reported to his supervisor. He told him about the phone call and his admissions concerning the inappropriate emails that he forwarded and his visits to

pornographic sites. After the investigation, a Report of Adverse Information was issued on June 1, 2005. (GE 1).

Applicant voluntarily sought counseling after his conversation with the IG office. He was concerned about any problems that he might have. He saw a military psychologist and psychiatrist at a naval hospital (AE NN). He also enrolled in an "Ethics in Cyberspace" course. After numerous counseling visits, Applicant received no diagnosis of any kind and no treatment or medications were prescribed (Tr 146).

At the hearing, Applicant explained he had not received security training about accessing unauthorized web sites. He acknowledged that he did sign Employee Handbook but did not read it. He realizes that is ono excuse for his behavior.

Applicant told his wife about the investigation and his use of the computer to visit and download pornographic sites. He had conversations with management and government personnel. He received a formal letter of reprimand and was put on a two-year probation with the written condition that any future infractions will result in immediate termination for cause (GE 1 at 2). He successfully completed his probation in 2007.

Applicant has rearranged his office. His computer is now in full sight so that the monitor is visible to all persons passing his door. He admits that he misused his NMCI technology system. His behavior in downloading pornographic material from the internet could put the intranet system in danger. He admits his judgment was poor, despite the fact that he was receiving the emails from other government personnel. Applicant did not really think that forwarding the emails was inappropriate since others in the company were sending the joke emails. He also was shown the pornographic sites by some of the personnel in company. He was adamant when testifying that he now knows it was inappropriate conduct and could jeopardize the security system. He was credible in his testimony that he would never repeat such conduct.

Applicant's work record with the defense contractor since November 2000 is exemplary in every respect. Several government, military, and company associates and superiors have lauded his superior efforts and expertise. His performance before and after the incident with the computer is flawless. He is competent and professional. His coworkers applaud him as a man of character. He continues to have access to sensitive privacy-act protected information. At the hearing, his supervisors and colleagues repeatedly praised him as having an impeccable work ethic; strong character, dependable, reliable, honest, trustworthy and willing to maintain policies established within the organization. (AE OO). His military record is replete with awards and commendations (AE A-LL). Each witness praised Applicant for his competence and integrity. In 2007, Applicant received another commendation from his employer for exemplary service (AE F).

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).[1] Decisions must also reflect consideration of the factors listed in ¶ 2(a) of the new guidelines.[2] The presence or absence of a disqualifying or mitigating condition 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[3] 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 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.[4] 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 as his or her own. 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.[5]

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

---

[1] Directive. 6.3.

[2] 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.

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

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

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

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, and 1.b. Further, the information presented requires application of the disqualifying condition listed at AG ¶ 40(e) (*unauthorized use of a government or other information technology system*).

In response to the SOR, Applicant has admitted his misuse of his government computer when he forwarded emails that contained nude photos of women, and when he visited and downloaded pornographic sites from at least 2003 until 2005.

The record supports consideration of the Guideline M mitigating conditions listed in 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*). This conduct was not recent. His last misuse was in 2005. Applicant has demonstrated through successful completion of his two-year probation and no further violations that his actions do not reflect adversely on his "reliability, trustworthiness, or good judgment." (AG ¶ 41(a)) Indeed, his actions show a willingness to gain psychiatric help and counseling to assure himself and the government that there was no other problem. He has received commendations since the incidents. His employer has recommended that he remain in his position. He has been open and honest with all involved. He is remorseful. He has taken a course on ethics. He is committed to his work and does not want to let his employer down. Any future transgressions will result in his termination.

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." Applicant may not be disqualified under Guideline E for the SOR ¶ 2.a allegation. The record shows that conduct is specifically covered under Guideline M and must be addressed according to AG ¶ 40(b), as discussed above.

However, even considering a personal conduct disqualification under Guideline E, Applicant has presented evidence of mitigation. Under Personal Conduct Mitigating Condition ¶17 (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*) Applicant has met his burden by taking the steps and actions that are discussed under Guideline M.

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).[6] Applicant is a mature adult whose recent job performance has been exemplary. He has maintained a security clearance for many years. His military record is replete with awards. He was open and honest about the joke emails that he received. At first, he did not realize the import of such emails, but he does not use that as an excuse. He took responsibility for his conduct, and he volunteered to seek counselling from the military psychiatrist and psychologist. His employer trusts him to maintain his assistant security position. He has rearranged his office computer so that anyone can see the display monitor anytime they pass his door. He was cooperative with his investigators. The record of behavioral change and rehabilitation is sufficient to show he is unlikely to repeat his conduct in the future. The record is sufficient to overcome the adverse information about Applicant's conduct. Applicant has mitigated the security concerns under misuse of technology and personal conduct.

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
Subparagraph 1.a:	For Applicant
Subparagraph 1.b:	For Applicant
Paragraph 2, Guideline E:	FOR APPLICANT
Subparagraph 2.a:	For Applicant

Conclusion

In light of all of the foregoing, it is clearly consistent with the national interest to grant Applicant eligibility for a security clearance. Eligibility for access to classified information is granted.

NOREEN A LYNCH
Administrative Judge

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