DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
----------	)	ISCR Case No. 07-06092
SSN: ----------	)	
	)	
Applicant for Security Clearance	)	

Appearances

For Government: D. Michael Lyles, Esquire, Department Counsel
For Applicant: *Pro Se*

February 28, 2008

Decision

LEONARD, Michael H., Administrative Judge:

Applicant contests the Defense Department's intent to deny or revoke his eligibility for an industrial security clearance. Acting under the relevant Executive Order and DoD Directive,[1] the Defense Office of Hearings and Appeals (DOHA) issued a statement of reasons (SOR) to Applicant on October 15, 2007. The SOR is equivalent to an administrative complaint and it details the factual basis for the action. The issues in this case fall under Guideline M for misuse of information technology systems and Guideline E for personal conduct, both of which are based on Applicant's misuse of a government computer at his place of work.

In addition, this case is brought under the revised Adjudicative Guidelines for Determining Eligibility for Access to Classified Information (Revised Guidelines) approved by the President on December 29, 2005. The Revised Guidelines were then modified by the Defense Department, effective September 1, 2006. They supersede or

[1] Executive Order 10865, *Safeguarding Classified Information within Industry*, dated February 20, 1960, as amended, and DoD Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program*, dated January 2, 1992, as amended (Directive).

replace the guidelines published in Enclosure 2 to the Directive. They apply to all adjudications and other determinations where an SOR has been issued on September 1, 2006, or thereafter.[2] The Directive is pending revision or amendment. The Revised Guidelines apply here because the SOR is dated after the effective date.

Applicant replied to the SOR on October 30, 2007, and requested a hearing. The hearing took place as scheduled on January 29, 2008, and the transcript (Tr.) was received on February 6, 2008.

The record was left open until February 15, 2008, to allow Applicant an opportunity to submit additional documentary evidence. Applicant timely submitted two letters vouching for his good character. The post-hearing exhibits were forwarded by department counsel who made no objections. The letters are marked and admitted as Exhibits E and F. For the reasons discussed below, this case is decided for Applicant.

Findings of Fact

Under Guideline M, the SOR alleges that in May 2006 Applicant's assigned government computer had inappropriate material on it in the form of "hacker tools" and adult-content material. Under Guideline E, the SOR cross-references the sole allegation under Guideline M. In his response to the SOR, Applicant admitted the factual allegations. Based on the record evidence as a whole, the following facts are established by substantial evidence.

Applicant is a 52-year-old employee for a company engaged in defense contracting. His educational background includes a bachelor of science in electrical engineering. He has worked for his current employer as a senior science advisor since October 2006 (Exhibit D). He was worked in the defense industry and held a security clearance for approximately the last 20 years. His current annual salary is about $120,000. Based on performance reviews covering 2003–2007, Applicant is a highly competent employee who produces high quality work (Exhibits A–D).

On Friday, May 19, 2006, an inspection discovered that Applicant's assigned government computer had inappropriate material on it in the form of "hacker tools" and adult-content material (Exhibit 3). Applicant was then an onsite company employee at a government facility and his computer was connected to the network system (Tr. 70-71). Applicant was escorted off the premises and interviewed. He reported that a computer disc—obtained at a military test facility—contained the "hacker tools" (Exhibit 3). Although Applicant's behavior was not in compliance with the rules for using a government computer, the Army Criminal Investigation Command (CID) determined that the incident was not a criminal matter and should be handled internally within the command. On Monday, May 22, 2006, Applicant returned to work at the company

[2] *See* Memorandum from the Under Secretary of Defense for Intelligence, dated August 30, 2006, Subject: Implementation of Adjudicative Guidelines for Determining Eligibility for Access to Classified Information (December 29, 2005).

location after he was orally reprimanded for not complying with established rules and was re-briefed on security issues. Applicant was specifically told that he violated a briefing he signed when he was given access to the computer and that he introduced software onto the computer without having it approved by the company program office (Exhibit 3 at 2). About a week later, he returned to the government facility where he worked until joining his current employer in October 2006.

Applicant addressed the May 2006 incident during his hearing testimony. He previously discussed the incident in April 2007 during an investigative interview (Exhibit 2). Concerning the "hacker tools," he explained it took place as part of his day-to-day work and it was not an attempt by him to hack the government computer system. He obtained the computer disc from another contractor who worked at a military test facility located in another state. The disc had a label that suggested to Applicant that it was appropriate to use it. Applicant understood the disc contained software to validate whether a computer system was secure (Tr. 68–70). Applicant took the disc back to his work location and attempted to use it. He did not load it onto his computer because he was not a system administrator (Tr. 71). Instead, he ran the program off the disc and immediately received a "hacker alert" alarm on his computer (Tr. 71–72). He shut the program down and placed the disc in an overhead bin where it remained until a few days later when the investigation commenced.

The ensuing investigation and audit of Applicant's computer discovered the "hacker tools" and adult-content material. Applicant agrees that he wrongfully used his government computer to access adult-content material. One of the Web sites he visited was for dating or match making (Tr. 74). He also admits that he visited this Web site on several occasions because he was curious, but he never acted on it. Based on this record, none of the Web sites involved nudity or sexually-explicit material.

Applicant has been married to the same woman since 1974. The couple have two adult children. His 31-year-old daughter is living on her own. His 23-year-old son is living at home recovering from a failed marriage and an unsuccessful college experience. Also, Applicant's mother-in-law is living with Applicant and his wife. His wife works as a secretary for transcription at a medical office.

Applicant's wife has never heard him discuss the nature of his work on behalf of the government. She became aware of the May 2006 incident when Applicant came home that day and told her about it. She described Applicant as her best friend, her rock, and they rely on each other for everything (Tr. 63).

In addition to his wife, a coworker presented favorable character evidence for Applicant. The coworker, a retired Army officer, has seen nothing of security significance during the 18 months he has worked with Applicant. He describes Applicant as a high-quality person who does high-quality work. In addition, the two post-hearing letters, one from a personal contact and the other from a professional contact, attest to Applicant's good character and suitability (Exhibits E and F).

Policies

This section sets forth the general principles of law and policies that apply to an industrial security clearance case. To start, no one has a right to a security clearance.[3] As noted by the Supreme Court in 1988 in the case of *Department of Navy v. Egan*, "the clearly consistent standard indicates that security clearance determinations should err, if they must, on the side of denials."[4] A favorable decision establishes eligibility of an applicant to be granted a security clearance for access to confidential, secret, or top-secret information.[5] An unfavorable decision (1) denies any application, (2) revokes any existing security clearance, and (3) prevents access to classified information at any level.[6] Under *Egan,* Executive Order 10865, and the Directive, any doubt about whether an applicant should be allowed access to classified information will be resolved in favor of protecting national security.

There is no presumption in favor of granting, renewing, or continuing eligibility for access to classified information.[7] The government has the burden of presenting evidence to establish facts alleged in the SOR that have been controverted.[8] An applicant is responsible for presenting evidence to refute, explain, extenuate, or mitigate facts that have been admitted or proven.[9] In addition, an applicant has the ultimate burden of persuasion to obtain a favorable clearance decision.[10] In *Egan*, the Supreme Court stated that the burden of proof is less than a preponderance of the evidence.[11] The agency appellate authority has followed the Court's reasoning, and a judge's findings of fact are reviewed under the substantial-evidence standard.[12]

The Revised Guidelines set forth adjudicative guidelines to consider when evaluating a person's security clearance eligibility, including disqualifying conditions

---

[3] *Department of Navy v. Egan*, 484 U.S. 518, 528 (1988) ("it should be obvious that no one has a 'right' to a security clearance"); *Duane v. Department of Defense*, 275 F.3d 988, 994 (10th Cir. 2002) ("It is likewise plain that there is no 'right' to a security clearance, so that full-scale due process standards do not apply to cases such as Duane's.").

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

[5] Directive, ¶ 3.2.

[6] Directive, ¶ 3.2.

[7] ISCR Case No. 02-18663 (App. Bd. Mar. 23, 2004).

[8] Directive, Enclosure 3, ¶ E3.1.14.

[9] Directive, Enclosure 3, ¶ E3.1.15.

[10] Directive, Enclosure 3, ¶ E3.1.15.

[11] *Egan*, 484 U.S. at 531.

[12] ISCR Case No. 01-20700 (App. Bd. Dec. 19, 2002) (citations omitted).

(DC) and mitigating conditions (MC) for each guideline. In addition, each clearance decision must be a fair and impartial commonsense decision based upon consideration of all the relevant and material information, the pertinent criteria and adjudication factors, and the whole-person concept. A person granted access to classified information enters into a special relationship with the government. The government must be able to have a high degree of trust and confidence in those persons to whom it grants access to classified information. The decision to deny a person a security clearance is not a determination of an applicant's loyalty.[13] Instead, it is a determination that the applicant has not met the strict guidelines the President has established for granting eligibility for a security clearance.

Analysis

Under Guideline M,[14] the security concern is that "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."[15]

The record evidence supports a conclusion that Applicant misused his government computer based on the May 2006 incident. Also, the record evidence supports application of two disqualifying conditions under Guideline M. First, by using the disc that contained the "hacker tools," Applicant introduced software onto an information technology system without proper authorization.[16] Second, Applicant engaged in the unauthorized use of a government computer by using it to access Web sites containing adult-content material.[17] Both matters raise a security concern and may be disqualifying because the matters call into question Applicant's reliability, trustworthiness, and good judgment.

Guideline M has three conditions that could mitigate the security concern, and those conditions are as follows:

---

[13] Executive Order 10865, § 7.

[14] Revised Guidelines at 26–27 (setting forth the mitigating and disqualifying conditions).

[15] Revised Guidelines at 26.

[16] DC 6 is the "introduction, removal, or duplication of hardware, firmware, software, or media to or from any information technology system without authorization, when prohibited by rules, procedures, guidelines, or regulations."

[17] DC 5 is the "unauthorized use of a government or other information technology system."

1. [S]o 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;

2. [T]he 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,

3. [T]he conduct was unintentional or inadvertent and was followed by a prompt, good-faith effort to correct the situation and by notification of supervisor.[18]

Each MC is discussed below.

The first MC applies to the "hacker tools" aspect of the May 2006 incident. It applies because the incident happened under circumstances where Applicant honestly believed that the disc he was using was appropriate given (a) how he came into possession of it and (b) his understanding of its purpose or function. These circumstances are unusual enough to suggest that a similar incident is unlikely to recur. It no longer casts doubt on his reliability, trustworthiness, or good judgment because this incident was an honest mistake. MC 1 does not, however, apply to the adult-content material aspect of the May 2006 incident.

The second MC applies to the "hacker tools" aspect of the May 2006 incident for two reasons. First, it applies because it was a minor incident in the scheme of things. The action taken against Applicant was limited to (a) losing a day of work when he was escorted off the premises and (b) an oral reprimand. This low-level action suggests that the matter was not viewed as a major or serious violation. Had the responsible authority viewed it otherwise, it is likely they would have taken more serious action—such as written reprimand, a multi-day suspension, or termination—against Applicant. Also, the fact that he returned to work at the government facility is probative. Had officials viewed the incident as a major violation, it is likely they would have banned Applicant from the government facility. Second, MC 2 applies because the reason Applicant used the disc on the government computer was because he believed, based on his visit to the military test facility, that the disc would help him with his work. Indeed, the evidence does not suggest Applicant was trying to hack into the system or engage in some other type of malicious behavior. Indeed, once he received the alarm, he immediately took the disc out and did not use it again. MC 2 does not, however, apply to the adult-content material aspect of the May 2006 incident.

The third MC does not apply to either aspect of the May 2006 incident. Although Applicant's introduction of the "hacker tools" onto the government computer was unintentional or inadvertent, he did not report that matter after receiving the alarm. Likewise, the adult-content material aspect does not qualify for mitigation under the plain language of this MC.

---

[18] Revised Guidelines at 26–27.

Under Guideline E,[19] the security concern is that "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."[20]

The record evidence raises a security concern under Guideline E, because Applicant's misuse of a government computer violated a briefing he had signed when he was given access to the computer and that he introduced software onto the computer without having it approved by the company program office (Exhibit 3 at 2). Given these circumstances, his misuse falls within the meaning of DC 6.[21] This raises a security concern and may be disqualifying because it calls into question Applicant's reliability, trustworthiness, and good judgment.

Guideline E has several mitigating conditions, but the only pertinent one is MC 3, which provides as follows:

> [T]he 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.[22]

MC 3 applies because, as explained above under the Guideline M discussion, his misuse is minor in the scheme of things and it no longer casts doubt on Applicant's reliability, trustworthiness, or good judgment. The record evidence shows Applicant received the equivalent of a slap-on-the-wrist for the misuse and was allowed to return to the government facility where he remained until he started his new job in October 2006.

This case has also been considered under the whole-person concept, as the record evidence is both disqualifying and mitigating. Applicant is 52 years old and sufficiently mature to make prudent decisions about his conduct at the work place. Overall, his misuse of the government computer was relatively minor. The "hacker tools" aspect of the May 2006 incident was a sloppy mistake, but also an honest mistake made without malice. The adult-content material aspect of the May 2006 incident was not an honest mistake, and Applicant admits he was wrong. The record evidence shows, however, that his actions in this regard did not involve nudity or sexually-explicit

---

[19] Revised Guidelines at 10–12 (setting forth the mitigating and disqualifying conditions).

[20] Revised Guidelines at 10.

[21] DC 6 is the "violation of a written or recorded commitment made by the individual to the employer as a condition of employment."

[22] Revised Guidelines at 11.

material, which would be considered a major or serious transgression. On this basis, it is mitigated. In addition, Applicant has approximately 20 years of work history in the defense industry, and his recent performance reviews establish that Applicant is a highly competent employee working in a highly technical field (Exhibits A–D). Based on this record, it appears the May 2006 incident is the only adverse information concerning Applicant. This circumstance suggests that Applicant has, on balance, the requisite self-control, good judgment, reliability, trustworthiness, and ability to properly handle and safeguard classified information. Finally, based on his testimony and demeanor during the hearing, Applicant appeared to be contrite. Accordingly, the likelihood of continuance or recurrence of similar conduct is assessed as remote if not nil.

Based on the record evidence as a whole, both favorable and unfavorable, Applicant presented sufficient evidence to explain, extenuate, or mitigate the security concerns under both guidelines. Applicant met his ultimate burden of persuasion to obtain a favorable clearance decision. This case is decided for Applicant.

Formal Findings

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

Paragraph 1, Guideline M:	For Applicant
Subparagraph 1.a:	For Applicant
Paragraph 2, Guideline E:	For Applicant
Subparagraph 2.a:	For Applicant

Conclusion

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

Michael H. Leonard
Administrative Judge