DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
----------	)	ISCR Case No. 03-17291
SSN: ----------	)	
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Candace Le'i, Esq., Department Counsel
For Applicant: Jonathan A Gowen, Esq.

November 20, 2008

_____

Decision

_____

FOREMAN, LeRoy F., Administrative Judge:

This case involves security concerns raised under Guidelines M (Use of Information Technology Systems) and E (Personal Conduct). Eligibility for access to classified information is denied.

Statement of the Case

Applicant submitted a security clearance application on November 19, 2002, and he was granted an interim clearance. On March 25, 2008, the Defense Office of Hearings and Appeals (DOHA) issued a Statement of Reasons (SOR) detailing the basis for its preliminary decision to deny his application, citing security concerns under Guidelines M and E. 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 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 Applicant's interim clearance was withdrawn in November 2007.

Applicant answered the SOR on April 28, 2008; and he requested a decision on the record without a hearing. After the File of Relevant Material was sent to Applicant, he retained an attorney. On September 3, 2008, his attorney requested a hearing. Department Counsel was ready to proceed on September 15, 2008, and the case was assigned to me on the same day. DOHA issued a notice of hearing on September 18, 2008, scheduling the hearing for October 16, 2008. I convened the hearing as scheduled. Government Exhibits (GX) 1 and 2 were admitted in evidence without objection. Applicant testified on his own behalf, and submitted Applicant's Exhibits (AX) A through E, which were admitted without objection. DOHA received the transcript (Tr.) on October 22, 2008.

I granted Department Counsel's request to keep the record open until October 27, 2008, to submit a memorandum of law pertaining to the statutes, regulations, directives, or rules that may have been violated by the conduct alleged under Guideline M. I received Department Counsel's memorandum on October 27, 2008, and Applicant's response to the memorandum on November 7, 2008. They are attached to the record as Hearing Exhibits I and II.

Procedural Matters

On my own motion, I amended SOR ¶ 1, without objection of either party, to insert the verb that was omitted from the second sentence. As amended, the word "include" is added after the third word of the second sentence (Tr. 10). The amendment is handwritten on the SOR.

Findings of Fact

In his answer to the SOR, Applicant admitted the allegations in SOR ¶¶ 1.a and 2.b. His admissions are incorporated in my findings of fact.

Applicant is a 35-year-old senior systems engineer employed by a federal contractor. He has worked for his current employer since November 2002. His duties involve installing and maintaining access control systems for government buildings (Tr. 23). He was married in November 1997, owns his home, and has three children, ages seven, three, and two.

Applicant applied for a job with a federal agency in 2002, and he disclosed his illegal file swapping to a security investigator (GX 2 at 2). On October 25, 2007, he submitted a signed and sworn statement to another security investigator in which he discussed his involvement in illegal file swapping (GX 2). He testified he was uncomfortable during this interview, but nothing in his sworn statement was untrue. He felt, however that some clarification of his statement was needed. He used his response to the SOR and his testimony at the hearing to clarify some parts of his statement (Tr. 27).

In his sworn statement, Applicant defined illegal file swapping as "downloading files or programs without paying for the license." He admitted illegal file swapping from 1993, when he was in college, until October 20, 2007, when he downloaded a serial number for a multimedia program and used it to unlock the program and view a movie trailer. The serial number would have cost $29.99 if purchased, but Applicant was able to download it without paying for it.

Applicant told the security investigator the computer sites he used were "too numerous to list." He admitted illegal file swapping about once a month, except for a six-month period of unemployment from May to November 2002, when he engaged in file swapping about twice a week. At the hearing, he testified he looked for files to download about once a month, but did not download something every month.

The materials illegally downloaded included anti-virus programs, word processing programs, games, movies, and miscellaneous study guides, certifications, "cheat sheets" for games, and manuals for products. He eventually purchased some of the movies and games he had downloaded. He estimated the total value of programs he had illegally downloaded to be between $750 and $1,000. He told the investigator he planned "to do less" illegal file downloading and he hoped that "someday" he would stop it completely. At the hearing, he testified he had not illegally downloaded anything since October 2007 and did not intend to do it again (Tr. 49).

Applicant testified he had never sold or profited from anything he downloaded (Tr. 34). He admitted that, even though the law in the early 1990s was "very gray," he knew "from a moral perspective" it was wrong to download programs without paying for them (Tr. 46).

In his statement, Applicant also admitted that in 1999 he and two coworkers stole computer equipment from a former employer while moving equipment to a different location. He did not know what his coworkers took, but he personally took four memory sticks worth $25 to $50 each, a central processing unit chip worth $100 to $120, and a video card worth $75 to $100. The equipment was old and not intended for further use by his employer (Answer at 2). In his answer to the SOR and at the hearing, Applicant stated he would not have stolen the equipment if his coworkers had not approached him with the idea and if the likelihood of getting caught had not been remote (Answer at 2; Tr. 50).

Applicant submitted performance appraisals from his current employer for his two previous rating periods. For the period ending in May 2008 (AX B), he was rated "outstanding" in independence; and "excellent" in technical skill, work quality, and dependability, on a five-level scale ranging from "outstanding" to "poor." For the period ending in November 2006 (AX A), he was rated "outstanding" in dependability and independence; and "excellent" in technical skill, work quality, and productivity. In August 2007, he was promoted to be an area operations manager (Tr. 36).

Applicant presented a statement from his director of operations (AX C), who described him as "a person of high moral character and judgment." A physical security specialist for the U.S. Secret Service who has worked with Applicant for two years considers him "a person worthy of trust and confidence," whose integrity has never been in question (AX D). Another Secret Service employee who has worked with Applicant for six years considers him trustworthy and reliable (AX E).

Applicant testified his current employer was aware of his file swapping activities but not the theft of computer equipment (Tr. 37). His supervisor's first reaction when informed of the illegal file sharing was "you've got to be kidding me," because his supervisor believed none of their employees would have a clearance if illegal file sharing were a disqualifying factor (Tr. 54).

Policies

"[N]o one has a 'right' to a security clearance." *Department of the Navy v. Egan*, 484 U.S. 518, 528 (1988). As Commander in Chief, the President has the authority to control access to information bearing on national security and to determine whether an individual is sufficiently trustworthy to have access to such information." *Id.* at 527. The President has 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. Or. 10865, *Safeguarding Classified Information within Industry* § 2 (Feb. 20, 1960), as amended and modified.

Eligibility for a security clearance is predicated upon the applicant meeting the criteria contained in the revised adjudicative guidelines (AG). These guidelines are not inflexible rules of law. Instead, recognizing the complexities of human behavior, these guidelines are applied in conjunction with an evaluation of the whole person. An administrative judge's over-arching adjudicative goal is a fair, impartial and common sense decision. An administrative judge must consider all available, reliable information about the person, past and present, favorable and unfavorable.

The government reposes a high degree of trust and confidence in persons with access to classified information. This relationship transcends normal duty hours and endures throughout off-duty hours. 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.

Clearance decisions must be "in terms of the national interest and shall in no sense be a determination as to the loyalty of the applicant concerned." *See* Exec. Or. 10865 § 7. Thus, a decision to deny a security clearance is not necessarily a determination as to the loyalty of the applicant. It is merely an indication the applicant has not met the strict guidelines the President and the Secretary of Defense have established for issuing a clearance.

Initially, the government must establish, by substantial evidence, conditions in the personal or professional history of the applicant that may disqualify the applicant from being eligible for access to classified information. The government has the burden of establishing controverted facts alleged in the SOR. *See Egan*, 484 U.S. at 531. "Substantial evidence" is "more than a scintilla but less than a preponderance." *See v. Washington Metro. Area Transit Auth.*, 36 F.3d 375, 380 (4th Cir. 1994). The guidelines presume a nexus or rational connection between proven conduct under any of the criteria listed therein and an applicant's security suitability. *See* ISCR Case No. 95-0611 at 2 (App. Bd. May 2, 1996).

Once the government establishes a disqualifying condition by substantial evidence, the burden shifts to the applicant to rebut, explain, extenuate, or mitigate the facts. Directive ¶ 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). "[S]ecurity clearance determinations should err, if they must, on the side of denials." *Egan*, 484 U.S. at 531; *see* AG ¶ 2(b).

Analysis

Guideline M, Use of Information Technology Systems

The SOR alleges Applicant "illegally downloaded software, serial numbers, games, study guides, manuals, and movies" from 1993 until "at least" October 20, 2007 (SOR ¶ 1.a); and that he intends to continue his illegal downloading (SOR ¶ 1.b). The security concern under this guideline is set out in AG ¶ 39 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.

Three disqualifying conditions under this guideline are potentially relevant. The disqualifying condition in AG ¶ 40(a) is raised by "illegal or unauthorized entry into any information technology system or component thereof." AG ¶ 40(c) is raised by "use of any information technology system to gain unauthorized access to another system or to a compartmented area within the same system." AG ¶ 40(f) is raised by "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." The phrase "any information technology system" indicates that this guideline applies to privately-owned systems as well as government

systems. *See* ISCR Case No. 99-0054, 2000 WL 1247735 (App. Bd. Jul. 24, 2000) (Guideline M covers misuse of government computers or private computers).

AG ¶¶ 40(a) and (c) both involve "unauthorized" entry or access. There is no evidence Applicant entered any system illegally or without authorization. Instead, it shows he entered systems available to the public, but was able to bypass the licensing requirements and download games, software, music, videos, and publications without paying for them. Thus, AG ¶¶ 40(a) and (c) are not raised.

The issue under AG ¶ 40(f) is whether Applicant downloaded and copied software or media "without authorization, when prohibited by rules, procedures, guidelines, or regulations." Department Counsel submitted no evidence of rules, procedures, guidelines, or regulations at the hearing, but she submitted a memorandum of law after the hearing, arguing that Applicant was guilty of copyright violations as well as larceny under state law. In response to Department Counsel's post-hearing submission, Applicant submitted a memorandum arguing that the government failed to prove a violation of any rules, procedures, guidelines, or regulations. Attached to Applicant's submission was a legal treatise tracing the changes in copyright law triggered by the widespread practice of downloading and recording media from the internet: Niels B. Schumann, *Direct Infringement on Peer-to-Peer Networks,* William Mitchell College of Law, Legal Studies Research Paper Series, Working Paper No. 9, April 2005, available at http://ssrn.com/abstract=703882 (hereinafter referred to as "Schumann").

The Copyright Act, 17 U.S.C. § 106, *et seq.*, vests certain exclusive rights in the owner of a copyright. The Act also recognizes that fair use of copyrighted material is not an infringement of the copyright. Fair use is not statutorily defined, except by illustrative examples, "such as criticism, comment, news reporting, teaching (including multiple copies for classroom work), scholarship, or research." 17 U.S.C. § 107. The development of the law regarding "fair use" is complex and evolving. In *A&M Records, Inc. v. Napster, Inc.,* 239 F.3d 1004 (9th Cir.2001), the Ninth Circuit affirmed a trial court decision that about 75 million users were infringing copyright by exchanging music files via a peer-to-peer network. *Napster* involved a network in which each user became a distributor because the user's computer became a server accessible to other users. Recording music for personal, noncommercial use is statutorily recognized as protected from infringement actions by the Audio Home Recording Act of 1992, 17 U.S.C. § 1008); *See* Schumann at 5. Similarly, recording movies on a videocassette recorder for personal, noncommercial use was recognized by the Supreme Court as fair use in *Sony Corporation of America v. Universal City Studios*, 464 U.S. 417, 442 (1984). *See* Schumann at 8-9.

The No Electronic Theft Act, 17 U.S.C. § 506, enacted in 1997, imposed criminal penalties for copyright infringement, if the infringement was "for purposes of commercial advantage or private financial gain" by the reproduction of one or more copies of copyrighted works during a 180 period with a total retail value of more than $1,000, or by distribution by making it available on a computer network accessible to the public,

knowing that it was intended for commercial distribution. Applicant admitted copying for "private financial gain," i.e., avoiding payment for the downloaded materials, but the total value of the materials fell short of the $1,000 threshold, and they were not made available on a computer network. Thus, his conduct did not violate the No Electronic Theft Act.

The record is sparse with respect to the circumstances surrounding much of Applicant's copying of materials from the internet, but he arguably was within the boundaries of "fair use" on some of his downloading and copying, except for those instances when he bypassed the licensing requirements. The Digital Millennium Copyright Act (DMCA), 17 U.S.C. § 1201, which became effective on November 29, 1999, provides, "No person shall circumvent a technological measure that effectively controls access to a work protected under this title." Applicant admitted that he circumvented the measures that required payment for many of the materials he downloaded. Thus, each time he circumvented the payment requirement between November 29, 1999 and October 20, 2007, his last admitted download, he violated the DMCA.

Department Counsel also argued that Applicant committed larceny under the law of the state in which he now resides. The statute cited, however, refers to "goods or merchandise of any store or other mercantile establishment." It also applies to only one of several states in which Applicant resided while downloading materials without paying for them. The state's computer crimes statute, not cited by Department Counsel, is devoted primarily to crimes in which a computer is used as a tool for committing other criminal offenses. In light of my conclusion that Applicant violated the DMCA, I find it unnecessary to determine whether he violated state law. Based on his violations of the DMCA, I conclude AG ¶ 40(f) is raised.

Since the government produced substantial evidence to raise the disqualifying condition in AG ¶ 40(f), the burden shifted to Applicant to produce evidence to rebut, explain, extenuate, or mitigate the facts. Directive ¶ E3.1.15. An applicant has the burden of proving a mitigating condition, and the burden of disproving it never shifts to the government. *See* ISCR Case No. 02-31154 at 5 (App. Bd. Sep. 22, 2005).

Among the enumerated mitigating conditions under this guideline, the only relevant mitigating condition is set out in AG ¶ 41(a): "[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." This mitigating condition requires an assessment of the likelihood of recurrence based on either the passage of time or the unusual circumstances surrounding the behavior. Even if recurrence is unlikely, this mitigating condition is not established unless the conduct does not cast doubt on the Applicant's reliability, trustworthiness, or good judgment.

The first prong of AG ¶ 41(a) ("so much time") is not established, because Applicant's last act of downloading material without paying for it was only a year before

his hearing, ending a span of about 15 years of downloading copyrighted material one or more times a month. The second prong ("unusual circumstances") is not established by the evidence. Regarding the likelihood of recurrence, Applicant told a security investigator in October 2007 that he intended to do less unauthorized downloading and "someday" would stop completely. At the hearing he declared he would not do it again. Based on his demeanor and all the evidence, I believe Applicant's declaration of intent at the hearing was honest and sincere, but it was motivated by his belated realization that continuing his unauthorized downloading could cost him his clearance. I am not convinced that he will not revert to old behavior when the pressure of obtaining a clearance is removed.

There is no evidence Applicant used a contractor-owned or government computer for his activities. All the downloading appears to have been off duty. The market value of the materials he downloaded is less than $1,000, spread over a 15-year period. The security significance of his conduct arises from its repetitive nature over a long period, and his awareness that each act was illegal. His conduct demonstrates an inability or unwillingness to follow rules; and it casts doubt about his reliability, trustworthiness, and good judgment. I conclude AG ¶ 41(a) is not established.

The SOR ¶ 1.b alleges Applicant intends to continue his illegal downloading. This allegation does not plead an independent basis for concern, but merely alleges intent to continue the disqualifying conduct alleged in SOR ¶ 1.a. As such, it pleads the absence of mitigation instead of an independent basis for concern. It also is rebutted by the evidence because, as noted above, Applicant honestly and sincerely intended as of the date of the hearing to discontinue his illegal downloading. Whether he will change his mind when he is relieved of the pressure of obtaining a clearance is a separate issue. I resolve SOR ¶ 1.b in Applicant's favor.

Guideline E, Personal Conduct

The SOR cross-alleges the Guideline M conduct under this guideline (SOR ¶ 2.a). In addition, it alleges that in 1999 he stole four memory sticks, a central processing unit chip, and a video card (SOR ¶ 2.b). The concern under this guideline is set out in AG ¶ 15 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."

Two potentially disqualifying conditions are relevant. The disqualifying condition in AG ¶ 16(c) is raised by "credible adverse information in several adjudicative issue areas that is not sufficient for an adverse determination under any other single guideline, but which, when considered as a whole, supports a whole-person assessment of questionable judgment, untrustworthiness, unreliability, lack of candor, unwillingness to comply with rules and regulations, or other characteristics indicating that the person may not properly safeguard protected information." AG ¶ 16(e) is raised by "personal conduct, or concealment of information about one's conduct, that creates a

vulnerability to exploitation, manipulation, or duress, such as . . . engaging in activities which, if known, may affect the person's personal, professional, or community standing." Applicant's 15-year record of intentionally circumventing the requirement to pay for downloaded materials, his 9-year record of violating the DMCA, and his theft of computer equipment in 1999 demonstrate an unwillingness to comply with rules and regulations, and are sufficient to raise AG ¶ 16(c). His theft of computer equipment and his concealment of that conduct from his current employer raise AG ¶ 16(e).

Security concerns under this guideline may be mitigated if "the 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." AG ¶ 17(c). Each copyright violation, and arguably even the theft of computer equipment, might be considered "minor" standing alone, but the repetitive nature of Applicant's conduct over a 15-year period negates a finding that it was infrequent. His conduct was recent and not the product of unusual circumstances. His repeated illegal conduct, knowing that it was illegal, casts doubt on his reliability, trustworthiness, and good judgment. For these reasons as well as the reasons set out above pertaining to AG ¶ 41(a) under Guideline M, I conclude AG 17(c) is not established.

Security concerns also may be mitigated if "the individual has taken positive steps to reduce or eliminate vulnerability to exploitation, manipulation, or duress." AG ¶ 17(e). Applicant has disclosed his unauthorized downloading to his supervisors, but he did not disclose his theft of computer equipment in 1999. I conclude this mitigating condition is established only for his unauthorized downloading.

Whole Person Concept

Under the whole person concept, an 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. An 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) 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.

Under AG ¶ 2(c), the ultimate determination of whether to grant eligibility for a security clearance must be an overall common sense judgment based upon careful consideration of the guidelines and the whole person concept. I have incorporated my comments under Guidelines M and E in my whole person analysis. Some of the factors

in AG ¶ 2(a) were addressed under those guidelines, but some warrant additional comment.

Applicant began his unauthorized downloading while in college, at a time when the law was unclear and file sharing was widespread and socially acceptable. He knew, or should have known, that his unauthorized downloading was an issue after he was interviewed about it by a security investigator in 2002. He continued it after receiving an interim clearance and did not stop until he was interviewed by a security investigator in October 2007. Even during that interview, he was noncommittal about changing his behavior. His comment to the investigator about hoping to stop illegal downloading completely suggests something akin to addiction.

Applicant is now 35 years old, married, a homeowner, a father of three children, gainfully employed, and highly respected by his peers, colleagues and supervisors. He is not an expert in copyright law. He held an interim clearance for almost six years, apparently without incident. There is no evidence he misused information systems owned by the government or his employer. There is no evidence of damage to information systems or harm to others, except for depriving some copyright owners of their royalties.

On the other hand, Applicant admitted knowing his conduct was wrong. He persisted in his conduct even though he knew after a security interview in 2002 that it raised security issues. He continued his illegal downloading while holding an interim clearance. His area of expertise is in access control systems. His lengthy history of knowingly and intentionally breaking the rules by misusing his expertise to bypass technological protection for copyrighted materials raises doubt about his ability and willingness to follow rules.

Applicant knowingly and intentionally violated the law every time he illegally bypassed a licensing agreement or otherwise failed to pay for software. He made a conscious choice not to obey the law, knowing that it was unlikely he would be found out, sued, prosecuted, or otherwise held accountable. His theft of computer parts from his employer suggests his vulnerability to peer pressure and willingness to act in self interest when detection is unlikely. He may have matured past his earlier susceptibility to peer pressure, but he continued his illegal downloading until recently, when he finally realized he would be held accountable for it. The high degree of trust and confidence implicit in a security clearance requires that an applicant be willing to follow the rules even when unsupervised and unlikely to be caught or sanctioned for violations.

After weighing the disqualifying and mitigating conditions under Guidelines M and E, and evaluating all the evidence in the context of the whole person, I conclude Applicant has not mitigated the security concerns based on use of information systems and personal conduct. Accordingly, I conclude he has not carried his burden of showing that it is clearly consistent with the national interest to grant him eligibility for access to classified information.

Formal Findings

I make the following formal findings for or against Applicant on the allegations set forth in the SOR, as required by Directive ¶ E3.1.25:

Paragraph 1, Guideline M (Information Technology):	AGAINST APPLICANT
Subparagraph 1.a:	Against Applicant
Subparagraph 1.b:	For Applicant
Paragraph 2, Guideline E (Personal Conduct):	AGAINST APPLICANT
Subparagraph 2.a:	Against Applicant
Subparagraph 2.b:	Against Applicant

Conclusion

In light of all of the circumstances, 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.

_____
LeRoy F. Foreman
Administrative Judge