DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
---	)	ISCR Case No. 15-03795
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Eric Borgstrom, Esquire, Department Counsel
For Applicant: *Pro se*

07/25/2016

Decision

GALES, Robert Robinson, Administrative Judge:

Applicant mitigated the security concerns regarding use of information technology systems, criminal conduct, and personal conduct. Eligibility for a security clearance and access to classified information is granted.

Statement of the Case

On August 12, 2014, Applicant applied for a security clearance and submitted an Electronic Questionnaire for Investigations Processing (e-QIP) version of a Security Clearance Application.[1] On December 1, 2015, the Department of Defense (DOD) Consolidated Adjudications Facility (CAF) issued a Statement of Reasons (SOR) to him, under Executive Order 10865, *Safeguarding Classified Information within Industry* (February 20, 1960), as amended and modified; DOD Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (January 2, 1992), as amended and modified (Directive); and the *Adjudicative Guidelines for Determining Eligibility For Access to Classified Information* (December 29, 2005) (AG) applicable to

[1] GE 1 (e-QIP, dated August 12, 2014).

all adjudications and other determinations made under the Directive, effective September 1, 2006.

The SOR alleged security concerns under Guidelines M (Use of Information Technology Systems), J (Criminal Conduct), and E (Personal Conduct), and detailed reasons why the DOD adjudicators were unable to find that it is clearly consistent with the national interest to grant or continue a security clearance for Applicant. The SOR recommended referral to an administrative judge to determine whether a clearance should be granted, continued, denied, or revoked.

Applicant received the SOR on December 11, 2015. In a sworn statement, dated December 22, 2015,[2] Applicant responded to the SOR allegations and requested a hearing before an administrative judge. Department Counsel indicated the Government was prepared to proceed on March 23, 2016. The case was assigned to me on April 4, 2016. A Notice of Hearing was issued on April 8, 2016. I convened the hearing as scheduled on April 27, 2016.

During the hearing, 2 Government exhibits (GE) 1 and 2, and 11 Applicant exhibits (AE) A through K, were admitted into evidence without objection. Applicant and one witness testified. The transcript (Tr.) was received on May 6, 2016. I kept the record open to enable Applicant to supplement it. Applicant took advantage of that opportunity. He timely submitted a number of documents which were marked as AE L through AE P, and admitted into evidence without objection. The record closed on May 18, 2016.

Findings of Fact

In his Answer to the SOR, Applicant admitted, with explanations, all of the factual allegations of the SOR, but denied the conclusions derived therefrom. Applicant's admissions and explanations are incorporated herein as findings of fact. After a complete and thorough review of the evidence in the record, and upon due consideration of same, I make the following additional findings of fact:

Applicant is a 27-year-old employee of a defense contractor who, since July 2011, has been serving as a research and development engineer.[3] He has never served in the U.S. military.[4] He was granted an interim top secret (TS) security clearance on an unspecified date about one year ago, but that security clearance was withdrawn over the current security concerns.[5] A 2007 high school graduate, Applicant received both a bachelor of science degree (in computer and systems engineering) and

[2] GE 1, *supra* note 1, at 12.

[3] GE 1, *supra* note 1, at 18.

[4] GE 1, *supra* note 1, at 25-26; Tr. at 45-46.

[5] GE 1, *supra* note 1, at 8.

a master of science degree (in computer science) in August 2011.[6] He has never been married.[7]

Use of Information Technology Systems, Criminal Conduct, & Personal Conduct

Over the years, Applicant has spent thousands of dollars on cable subscriptions, movies, and other intellectual property.[8] However, between the period from October 2010 to November 2014, Applicant also downloaded approximately 200 to 300 music files, network television shows, or movies from various sources on the internet to his personal computer. He estimated that 50 to 100 of the downloaded files were for television shows.[9] He generally watched one particular subscription television series at a friend's residence, and on a few occasions when the friend was away, Applicant downloaded several episodes of that series. He subsequently purchased the entire series.[10] The majority of the downloads occurred while Applicant was in college and for a relatively brief period thereafter. After July 2011, the downloaded materials consisted primarily of music and network television shows.[11] He last downloaded music and movies in 2011 or 2012, and network television shows in mid-2015.[12]

Applicant never uploaded or posted any of the downloaded videos, television shows, or music files on the internet, and he never shared his downloaded files on any peer-to-peer (P2P) networks. He may have shared some of the downloaded music files with his college roommate. He never made copies of the downloaded files. He never downloaded or made copies of any propriety software programs.[13] There is no evidence that criminal charges were ever brought against Applicant, that civil complaints or copyright infringement actions were ever lodged against him, or that his employer ever disciplined him for misuse of information technology systems.[14]

Although the Government alleged that Applicant's downloading activities were criminal in nature, it failed or chose not to identify any particular law that Applicant may

---

[6] GE 1, *supra* note 1, at 11; GE 2 (Personal Subject Interview, dated November 4, 2014), at 3; AE H (Resume, undated); AE J (Extract of U.S. Office of Personnel Management (OPM) Report of Investigation, dated December 1, 2014).

[7] GE 1, *supra* note 1, at 20.

[8] AE M (Opening Statement, undated); AE F (Entertainment Expenses, various dates); AE G (Photo, undated).

[9] Tr. at 34-35.

[10] AE K (Corrections to GE 2, undated); Tr. at 38-39.

[11] Tr. at 35-37.

[12] Tr. at 44; AE M, *supra* note 8.

[13] Tr. at 35-38.

[14] Tr. at 55-58.

have violated, except during the closing argument phase of the hearing.[15] The senior director of computer vision at Applicant's employer likewise concluded that Applicant's downloading activities were illegal.[16] While Applicant initially acknowledged that his actions were illegal, his subsequent explanations regarding his actions and the motivations for those actions appear to support the opposite conclusion. He contended that, at the time of his downloading activities, he did not fully understand the impact of what he was doing under the law and that he has subsequently matured considerably and now fully appreciates that his actions were wrong. He ceased all such activities.[17]

Applicant's downloading activities were not for the purposes of commercial advantage or private financial gain; he did not download or reproduce for distribution one or more copies of any copyrighted works during a 180-day period with a total estimated retail value of more than $1,000; and he did not make any of the downloaded files available on a computer network accessible to the public, knowing that it was intended for commercial distribution.[18] The Government offered no evidence to contradict those facts. Thus, there is no evidence that Applicant's activities violated the No Electronic Theft Act.[19] Additionally, recording music for personal, noncommercial use is statutorily recognized as protected from infringement actions by the Audio Home Recording Act of 1992.[20] Similarly, recording or downloading movies on a videocassette recorder (or onto one's personal computer) for personal, noncommercial use is considered fair use.[21]

Applicant's use of his personal computer for anything other than work-related controlled, unclassified information is not subject to any blanket company prohibitions. Corporate policy procedures and prohibitions relate only to services furnished to the DOD.[22] Applicant's downloading of music files, network television shows, or movies from the internet to his personal computer, had no relationship to any DOD contract.

[15] During the closing argument phase of the hearing, Department Counsel raised the applicability of the Digital Millennium Copyright Act (DMCA), 17 U.S.C. § 1201 *et seq.* (November 29, 1999), which provides, in part, "No person shall circumvent a technological measure that effectively controls access to a work protected under this title." Department Counsel argued that Applicant obtained private financial gain when he obtained media, without further description or specificity, as to the technological measure that was supposedly circumvented, for which he was not paying. Tr. at 77. He also referred to a provision of the state penal code that discusses petit larceny. He referred to a hearing office decision by another administrative judge. Tr. at 78.

[16] AE A (Character Reference, dated December 21, 2015), at 2.

[17] AE E (Answer to the SOR, dated December 22, 2015), at 1.

[18] AE E, *supra* note 17, at 1; Tr. at 49.

[19] No Electronic Theft Act, 17 U.S.C. § 506 (Dec. 16, 1997). For an exhaustive discussion of the Act as well as other relevant legislation and judicial decisions, *see* Niels B. Schaumann, *Direct Infringement on Peer-to-Peer Networks*, William Mitchell College of Law, Legal Studies Research Paper Series, Working Paper No. 9 (April 2005).

[20] Audio Home Recording Act of 1992, 17 U.S.C. §§ 1001-1010.

[21] *Sony Corporation of America v. Universal City Studios*, 464 U.S. 417, 442 (1984).

[22] AE L (E-mail, dated May 13, 2016).

Character References and Work Performance

Applicant's senior director of computer vision has known Applicant since July 2011. During the period Applicant had an interim TS security clearance, there have been no concerns expressed by anyone related to his handling of classified information. Applicant is considered an introspective intellectual with deep technical skills. He is considered to be completely trustworthy. Applicant exhibits a "strict adherence to the rules about security as well as unclassified information systems at work." Applicant's downloading behavior is considered a "holdover from his youth, developed in an environment where such activities were very common and not viewed as breaking the law, unethical of otherwise discouraged." It is not believed that Applicant's downloading "indiscretions" extend in any way to more serious misuse of information systems, and Applicant is fully expected to strictly comply with all laws regarding media downloading and copyrights. He strongly supports granting Applicant a security clearance.[23]

The company information systems security manager, who also serves as a technical expert, opined that Applicant has at all times, "conducted himself responsibly and appropriately regarding [company] rules and procedures dealing with classified data."[24] A technical leader, under whom Applicant served, considers Applicant to be trustworthy and diligent. He does not consider Applicant to be a rule-violator.[25] Applicant's employee evaluations over the years generally refer to his "demonstrated hard work, dedication, responsibility and independence in getting the job done," as well as the fact that he has proven to be "one of the more valuable and sought-after members in the group."[26]

Policies

The U.S. Supreme Court has recognized the substantial discretion of the Executive Branch in regulating access to information pertaining to national security emphasizing, "no one has a 'right' to a security clearance."[27] 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. The President has authorized the Secretary of Defense or his designee to grant an applicant eligibility for access to classified information "only upon a finding that it is clearly consistent with the national interest to do so."[28]

[23] AE A, *supra* note 14, at 2.

[24] AE B (Character Reference, dated December 16, 2015).

[25] Tr. at 63-66.

[26] AE D (Employee Evaluations, various dates). The specific quotes are from the evaluation dated March 21, 2014.

[27] *Department of the Navy v. Egan*, 484 U.S. 518, 528 (1988).

[28] Exec. Or. 10865, *Safeguarding Classified Information within Industry* § 2 (Feb. 20, 1960), as amended and modified.

When evaluating an applicant's suitability for a security clearance, the administrative judge must consider the AG. In addition to brief introductory explanations for each guideline, the AG list potentially disqualifying conditions and mitigating conditions, which are used in evaluating an applicant's eligibility for access to classified information.

An administrative judge need not view the guidelines as inflexible, ironclad rules of law. Instead, acknowledging the complexities of human behavior, these guidelines are applied in conjunction with the factors listed in the adjudicative process. The administrative judge's overarching adjudicative goal is a fair, impartial, and commonsense decision. The entire process is a conscientious scrutiny of a number of variables known as the "whole-person concept." The administrative judge must consider all available, reliable information about the person, past and present, favorable and unfavorable, in making a meaningful decision.

In the decision-making process, facts must be established by "substantial evidence."[29] The Government initially has the burden of producing evidence to establish a potentially disqualifying condition under the Directive, and has the burden of establishing controverted facts alleged in the SOR. Once the Government has produced substantial evidence of a disqualifying condition, under Directive ¶ E3.1.15, the applicant has the burden of persuasion to present evidence in refutation, explanation, extenuation or mitigation, sufficient to overcome the doubts raised by the Government's case. The burden of disproving a mitigating condition never shifts to the Government.[30]

A person who seeks access to classified information enters into a fiduciary relationship with the Government predicated upon trust and confidence. This relationship transcends normal duty hours and endures throughout off-duty hours as well. It is because of this special relationship that 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. Decisions include, by necessity, consideration of the possible risk the applicant may deliberately or inadvertently fail to 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. Furthermore, "security clearance determinations should err, if they must, on the side of denials."[31]

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."[32] Thus, nothing

[29] "Substantial evidence [is] such relevant evidence as a reasonable mind might accept as adequate to support a conclusion in light of all contrary evidence in the record." ISCR Case No. 04-11463 at 2 (App. Bd. Aug. 4, 2006) (citing Directive ¶ E3.1.32.1). "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).

[30] *See* ISCR Case No. 02-31154 at 5 (App. Bd. Sep. 22, 2005).

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

[32] *See* Exec. Or. 10865 § 7.

in this decision should be construed to suggest that I have based this decision, in whole or in part, on any express or implied determination as to Applicant's allegiance, loyalty, or patriotism. It is merely an indication the Applicant has or has not met the strict guidelines the President and the Secretary of Defense have established for issuing a clearance. In reaching this decision, I have drawn only those conclusions that are reasonable, logical, and based on the evidence contained in the record. Likewise, I have avoided drawing inferences grounded on mere speculation or conjecture.

Analysis

Guideline M, Information Technology Systems

The security concern under the guideline for Use of Information Technology Systems is set out in AG ¶ 39:

> 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.

The guideline notes several conditions that could raise security concerns. Under AG ¶ 40(a), security concerns may be raised by the "illegal or unauthorized entry into any information technology system or component thereof." Similarly, under AG ¶ 40(c), the "use of any information technology system to gain unauthorized access to another system or to a compartmented area within the same system" may raise security concerns. Under AG ¶ 40(f), it is also potentially disqualifying if there is any "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 Appeal Board has previously ruled that "the language in [Guideline] M is broad enough to cover misuse of government computers or private computers.[33]

There is no allegation or evidence presented that Applicant ever gained illegal or unauthorized entry into either his company computer or his own personal computer. There were no government computers involved in any of his downloading activities. Although argued, Department Counsel submitted no evidence, except for Applicant's seemingly retracted admissions, that Applicant's downloading activities were illegal. He downloaded music files, network television shows, or movies from various sources on the internet to his personal computer. Those activities were not addressed in his

[33] ISCR Case No. 99-0554 at 4 (App. Bd. Jul. 24, 2000). It should be noted that the version of the AG considered in that decision was not the same as the current version, but was, in fact, the version issued on November 10, 1998. While the versions are not identical in content or structure, and there are differences in the specific language used, there are sufficient similarities to convey the establishment of similar policy in the 2006 version.

employer's rules, procedures, guidelines, or policies. The sole evidence reflecting any illegal activity by Applicant consists of his seemingly retracted admissions, and Department Counsel's suppositions that those activities must have been illegal for at least some of the downloaded materials because Applicant did not pay for them. There was no evidence presented that particular files were protected by any technological measures to effectively control access to those works. Without evidence pertaining to those technological measures, there is no evidence of a violation of the DCMA. Simply arguing that laws must have been violated, without connecting the specific activity (with particular attention to which music files, network television shows, or movies) to the specific law, is insufficient. Neither the No Electronic Theft Act nor the Audio Home Recording Act of 1992 was violated. Recording or downloading movies on a videocassette recorder or onto one's personal computer for personal, noncommercial use is considered fair use unless proven otherwise. Simply arguing that the activity constituted petit larceny under state law is insufficient. AG ¶¶ 40(a), 40(c), and 40(f) have not been established.

Guideline J, Criminal Conduct

The security concern relating to the guideline for Criminal Conduct is set out in AG ¶ 30: "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."

The guideline notes several conditions that could raise security concerns. Under AG ¶ 31(a), "a single serious crime or multiple lesser offenses" is potentially disqualifying. Similarly, under AG ¶ 31(c), if there is an "allegation of criminal conduct, regardless of whether the person was formally charged, formally prosecuted or convicted," security concerns may be raised. Applicant's alleged history of criminal conduct, during the period October 2010 to November 2014, consisted of his downloading music files, network television shows, or movies from various sources on the internet to his personal computer. Applicant never uploaded or posted any of the downloaded videos, television shows, or music files on the internet, and he never shared his downloaded files on any P2P networks. He never made copies of the downloaded files. He never downloaded or made copies of any proprietary software programs. There is no evidence that criminal charges were ever brought against Applicant, that civil complaints or copyright infringement actions were ever lodged against him. The majority of the downloads occurred while Applicant was in college and for a relatively brief period thereafter. In the absence of evidence, as opposed to merely argument, reflecting criminal conduct, the government did not establish by substantial evidence that Applicant's actions are criminal violations. AG ¶¶ 31(a) and 31(c) have not been established.

Guideline E, Personal Conduct

The security concern for Personal Conduct is set out in AG ¶ 15:

> 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.

The guideline notes a condition that could raise security concerns. Under AG ¶ 16(c), security concerns may be 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.

The alleged personal conduct behavior consisted of Applicant downloading music files, network television shows, or movies from various sources on the internet to his personal computer during the period October 2010 to November 2014, while he was in college and for a brief period thereafter. The evidence is not in dispute. Applicant acknowledged his downloading activities. He contended that, at the time of those downloading activities, he did not fully understand the impact of what he was doing under the law and that he has subsequently matured considerably and now fully appreciates that his actions were wrong. He ceased all such activities before the SOR was issued. AG ¶ 16(c) has not been established.

Whole-Person Concept

Under the whole-person concept, the 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. The 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 commonsense judgment based upon careful consideration of the guidelines and the whole-person concept. Moreover, I have

evaluated the various aspects of this case in light of the totality of the record evidence and have not merely performed a piecemeal analysis.[34]

The mitigating evidence under the whole-person concept is substantial. Applicant is considered an introspective intellectual with deep technical skills. He is considered to be completely trustworthy. He exhibits a "strict adherence to the rules about security as well as unclassified information systems at work." Applicant's downloading behavior is considered a "holdover from his youth, developed in an environment where such activities were very common and not viewed as breaking the law, unethical of otherwise discouraged." He no longer downloads any music files, network television shows, or movies from various sources on the internet to his personal computer, and has not done so for a substantial period. With his added maturity, the alleged behavior is unlikely to recur. Under the evidence presented, I have no questions about Applicant's reliability, trustworthiness, and ability to protect classified information. *See* AG ¶ 2(a)(1) through AG ¶ 2(a)(9).

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 M:	FOR APPLICANT
Subparagraph 1.a:	For Applicant
Paragraph 2, Guideline J:	FOR APPLICANT
Subparagraph 2.a:	For Applicant
Paragraph 3, Guideline E:	FOR APPLICANT
Subparagraph 3.a:	For Applicant

Conclusion

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

ROBERT ROBINSON GALES
Administrative Judge

[34] *See U.S. v. Bottone*, 365 F.2d 389, 392 (2d Cir. 1966); *See also* ISCR Case No. 03-22861 at 2-3 (App. Bd. Jun. 2, 2006).