DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 10-07794
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Tovah A. Minster, Esq., Department Counsel
For Applicant: *Pro se*

June 29, 2011

Decision

NOEL, Nichole L., Administrative Judge:

Applicant contests the Defense Department's intent to deny his eligibility for a security clearance to work in the defense industry. In 2007, Applicant resigned, in lieu of termination, from his employment with a government contractor because he misused the employer's computer system. Applicant presented evidence that he understands the nature and seriousness of his conduct and has not engaged in similar conduct in almost four years. Clearance is granted.

Statement of the Case

Acting under the relevant Executive Order and DoD Directive,[1] on January 13, 2011, the Defense Office of Hearings and Appeals (the Agency) issued a Statement of Reasons (SOR) explaining that it was not clearly consistent with the national interest to

[1] This case is adjudicated under Executive Order (EO) 10865, *Safeguarding Classified Information within Industry*, signed by President Eisenhower on February 20, 1960, as amended, as well as DoD Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program*, dated January 2, 1992, as amended (Directive). In addition, the *Adjudicative Guidelines for Determining Eligibility for Access to Classified Information* (AG), effective within the Defense Department on September 1, 2006, apply to this case. The AG were published in the Federal Register and codified in 32 C.F.R. § 154, Appendix H (2006). The AG replaces the guidelines in Enclosure 2 to the Directive.

grant Applicant access to classified information. The SOR detailed the factual basis for the action under security guidelines M (Use of Information Technology Systems) and E (Personal Conduct).

Applicant answered the SOR and requested a decision without a hearing. Department Counsel submitted the Government's written case on March 4, 2011. A complete copy of the file of relevant material (FORM) was provided to Applicant, who was afforded an opportunity to file objections and submit material to refute, extenuate, or mitigate the security concerns. Applicant received the FORM on March 18, 2011. He did not object to the items appended to the Government's brief. These documents are admitted as identified in the FORM as Items 1 though 6.

Applicant submitted a response to the FORM. Department Counsel did not object. As a result, it is admitted as Applicant's Exhibit (AE) A.

The case was assigned to me on May 5, 2011.

Findings of Fact

Applicant is a 32-year-old employee of a defense contractor who works as a software engineer. He has been employed with this company since 2008.[2]

Between 2002 and 2007, Applicant worked as a software engineer with a different government contracting company. His former employer had a very strict internet policy, which blocked employees from accessing their personal email accounts, as well as popular internet and social networking sites. Frustrated by the policy, Applicant admits that starting in 2004 he improperly used his employer's software and computer system to create a secure "tunnel" to his home computer in order to circumvent the company's firewall. This tunnel allowed him to access prohibited sites from his workstation through his home computer without compromising the company's network.[3]

Impressed by his accomplishment, Applicant admits he bragged about his actions on his MySpace page. In his posts, he named his employer and confirmed his status as an active employee. He disclosed that he internally circumvented the company's intranet firewall. He also disclosed that he had illegally downloaded thousands of copyrighted songs and one to two dozen movies from the internet onto his personal computer. Although it is unknown how his employer learned of the postings, Applicant was confronted by the human resources director in July 2007. Applicant admitted the allegations and was suspended for five days. At the end of his suspension, the human resources director informed Applicant that he was being terminated. He

[2] Item 5.

[3] Items 5-6; Response to FORM.

asked if he could resign in lieu of termination, and his employer agreed. After his initial confrontation by his employer, Applicant removed the MySpace postings.[4]

In the aftermath of his resignation, Applicant admits that while he understood that he violated company policy, he did not understand why, if no harm was done, his actions caused such a problem. Reflecting on his actions, Applicant cites his divorce as an aggravating factor. Going through a divorce, at 28 years old, after only two years of marriage, depressed him. He began to experience low self-esteem, which ultimately caused him to behave immaturely. At the time, he thought his MySpace posts made him look "cool" and the postings provided a boost to his ego. Now, Applicant sees that his behavior was wrong, immature, and dangerous. He understands that he placed himself and his former employer in a potentially compromising and vulnerable position. Since then, he has taken a more serious approach to security. He also sees a therapist regularly to deal with the issues stemming from his divorce.[5]

In the four years since he resigned from his former employer, he has not misused information technology systems entrusted to him by his subsequent employers. Nor has he committed any security violations. Since 2008, Applicant has not illegally downloaded copyrighted materials. He only purchases music and movies from legal on-line retailers.[6]

Policies

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

These guidelines are not inflexible rules of law. Instead, recognizing the complexities of human behavior, administrative judges apply the guidelines in conjunction with the factors listed in the adjudicative process. The administrative judge's overarching adjudicative goal is a fair, impartial, and commonsense decision. According to AG ¶ 2(c), 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 decision.

The protection of the national security is the paramount consideration. AG ¶ 2(b) requires that "[a]ny doubt concerning personnel being considered for access to classified information will be resolved in favor of national security." In reaching this

[4] Item 6.

[5] Items 4, 6.

[6] Response to FORM.

decision, I have drawn only those conclusions that are reasonable, logical, and based on the evidence.

Under Directive ¶ E3.1.14, the Government must present evidence to establish controverted facts alleged in the SOR. Under Directive ¶ E3.1.15, the applicant is responsible for presenting "witnesses and other evidence to rebut, explain, extenuate, or mitigate facts admitted by the applicant or proven by Department Counsel." The applicant has the ultimate burden of persuasion to obtain a favorable security decision.

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. The Government reposes a high degree of trust and confidence in 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 of potential, rather than actual risk of compromise of classified information.

Section 7 of EO 10865 provides that adverse decisions shall be "in terms of the national interest and shall in no sense be a determination as to the loyalty of the applicant concerned." *See also* EO 12968, Section 3.1(b) (listing multiple prerequisites for access to classified or sensitive information).

Analysis

Guideline M, Use of Information Technology Systems

The security concern 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 inability 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, however, only AG ¶¶ 40(b) and (e) apply. Applicant admits that between 2004 and 2007, he manipulated software available on his work computer to access his home computer allowing him to circumvent his employer's firewall and access otherwise restricted websites from his work computer. His actions constitute an " . . . unauthorized modification [or] manipulation . . . of access to information software, firmware, or hardware in an information system technology," under AG ¶ 40(b). His actions are also

disqualifying under AG ¶ 40(e) as an unauthorized use of a government or other information technology system.

Of the three mitigating conditions available under AG ¶ 41, one is applicable:

> (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.

Applicant's last known misuse of an information technology system occurred four years ago. Furthermore, he engaged in this behavior while going through a difficult divorce, which caused him to act out. Since then, he has seen the errors of his ways. Applicant's statements show he understands the security risk created by his behavior and that he will not engage in similar activity in the future. He has stated a commitment to security practices, as well as, respecting the integrity of the information systems to which he now has access.

While I cannot make a credibility determination of Applicant because I have not had the chance to observe him in person, I make the following observations of the record, which tend to support a finding in favor of Applicant's security worthiness. He self-reported his conduct on his security clearance applications. He reported his resignation in lieu of termination and the offenses leading to his resignation. He has been candid about his actions. He admitted the allegations of misconduct when confronted by his employer and has continued to do so. He takes responsibility for his actions. He has repeatedly expressed remorse for his behavior. These themes are consistent in his security clearance applications, his responses to Agency interrogatories, his Answer, and his FORM response. Also, in taking responsibility for his actions he is able to specifically identify several potential risks caused by his actions, which shows that he understands the nature and seriousness of his conduct. Finally, he is in therapy to deal with the issues of low self-esteem caused by his divorce. Viewed in its totality, these factors contribute to my favorable evaluation of Applicant's written statements.

While Applicant's past actions were serious, he has shown a more mature and responsible attitude leading me to conclude that he will not commit such actions in the future and that his past actions do not reflect negatively on his current reliability, trustworthiness, or good judgment.

Guideline E, Personal Conduct

AG ¶ 15 explains why personal conduct is a security concern:

> 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 SOR alleges that Applicant's resignation in lieu of termination raises questions about his security worthiness. I find that this is not disqualifying under AG ¶ 15. Applicant's resignation is a consequence of his misuse of his former employer's information systems. Applicant properly disclosed his resignation in lieu of termination on his security clearance application and offered an accurate explanation for the circumstances. However, his underlying actions are disqualifying under the general concern raised in AG ¶ 15. The security concerns raised by Applicant's misuse of his employer's information system is more appropriately addressed under Guideline M.

Applicant's admission that he illegally downloaded music and movies from the internet over a period of years cannot be ignored. His admission is credible adverse information in another issue area (in this case Guideline J, Criminal Conduct) 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 under AG ¶ 16(c).

Applicant's MySpace posts about misuse of his employer's information systems and his illegal downloading of copyrighted material raises significant questions about his judgment, reliability, trustworthiness and ability to protect classified information. Although these actions are not explicitly covered under any other guideline, when combined with all available information, they support 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 under AG ¶ 16(d).

Of the mitigating conditions available under AG ¶17, only the following is relevant:

17(c) the offense is so minor, or so much time has passed, 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.

In mitigating Applicant's illegal downloading of copyrighted material, I find Applicant illegally downloaded copyrighted material to his personal computer for his own use. There is no indication that he distributed any of the material he illegally obtained. While he did not believe so at the time, Applicant appreciates the security concern raised by illegally downloading copyrighted material. He now uses only legally acceptable methods to obtain copyrighted material from the internet. Given his change in behavior and attitude, I find that his past conduct does not cast doubt on his current reliability, trustworthiness, or good judgment.

Although Applicant's MySpace boasts cannot be considered minor lapses of judgment, I find that the conduct is mitigated for many of the same reasons as discussed in my analysis of AG ¶ 41(a).

When viewing the record as a whole, I have no reservations about Applicant's current reliability, trustworthiness, and ability to protect classified information. I considered the potentially disqualifying and mitigating conditions in light of all the facts and circumstances surrounding this case. In doing so, I have also considered the whole-person concept in my analysis of the applicable mitigating conditions and find a favorable conclusion is warranted.

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
Subparagraphs 1.a.:	For Applicant
Paragraph 2, Guideline E:	FOR APPLICANT
Subparagraphs 2.a. – 2.c.:	For Applicant

Conclusion

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

_____
Nichole L. Noel
Administrative Judge