DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
----------	)	ISCR Case No. 14-04650
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Andrew Henderson, Esquire, Department Counsel
For Applicant: *Pro se*

May 12, 2016

DECISION

ROSS, Wilford H., Administrative Judge:

Applicant submitted his Electronic Questionnaire for Investigations Processing (e-QIP), on February 12, 2014. (Government Exhibit 1.) On December 8, 2014, the Department of Defense issued a Statement of Reasons (SOR) detailing the security concerns under Guidelines M (Use of Information Technology Systems) and E (Personal Conduct) concerning Applicant. 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) effective within the Department of Defense on September 1, 2006.

Applicant answered the SOR in writing on December 22, 2014 (Answer), and requested a hearing before an administrative judge. Department Counsel was prepared to proceed on August 23, 2015. This case was assigned to me on September 1, 2015. The Defense Office of Hearings and Appeals (DOHA) issued a notice of hearing on September 15, 2015. I convened the hearing as scheduled on October 20, 2015. The Government offered Government Exhibits 1 and 2, which were admitted without objection. Applicant testified on his own behalf, and called two additional witnesses.

Applicant asked that the record remain open until November 13, 2015, for the receipt of documents. On October 28, 2015, Applicant submitted Applicant Exhibit A which was admitted without objection. DOHA received the transcript of the hearing (Tr.) on October 29, 2015. The record closed on November 13, 2015. Based upon a review of the pleadings, exhibits, and testimony, eligibility for access to classified information is granted.

Findings of Fact

Applicant is 28 and single. He has a master's degree in electronic engineering, is employed by a defense contractor in the computer security field, and seeks to retain a security clearance in connection with his employment.

Paragraph 1 (Guideline M, Use of Information Technology Systems)

Paragraph 2 (Guideline E, Personal Conduct)

The Government alleges under Guideline M that Applicant engaged in conduct that is in noncompliance with rules, procedures, guidelines, or regulations pertaining to information technology systems. The Government further alleges under Guideline E at allegation 2.a that Applicant's conduct under Guideline M shows questionable judgment, dishonesty, or an unwillingness to comply with rules and regulations. Applicant admitted allegation 1.a, with explanation. He denied allegations 1.b, and 2.a.

1.a. It is alleged in this subparagraph that Applicant was involved in knowingly and improperly being involved in a computer security incident in August 2013. The evidence shows that Applicant was acting under the direction of one of his instructors in college.

Applicant received his master's degree in 2013, with an emphasis on computer security. During that year he was working for one of his instructors, who has a private computer security business. In the summer of 2013, the instructor was contacted by a government organization for his help concerning a serious computer security incident. The instructor asked Applicant to assist in the investigation by looking at a particular computer function. During his investigation, which was extensive and highly technical, Applicant reached a point where he was uncertain of the legal implications of his continued work, so he stopped and contacted the instructor for advice on how to proceed. (Tr. 26-37, 39.)

Applicant's instructor provided a letter concerning this incident. The instructor confirmed that Applicant was working for him on the computer security incident, and confirmed Applicant's statements concerning the actions he took. The instructor then described what happened next, "He [Applicant] had stopped before proceeding too [far] into that [investigation of the computer function] and asked me how to proceed. Additional research may have required more aggressive probing that would potentially

require law enforcement approval. I sought such approval and at the time it was not desired." (Applicant Exhibit A at 3.)

1.b. The second incident alleged in the SOR is that Applicant knowingly engaged in a computer security violation by bringing a thumb drive from home and using it on his employer's computer system. Such conduct is alleged to be against company policy.

Applicant admitted the action, but stated that his conduct was not inappropriate, given his position in the company and the company's own rules. (Tr. 21-26.) The evidence supports his statements.

Applicant is employed as a "Network Engineer" by the company involved in this allegation. He provided documentation proving that fact. (Applicant Exhibit A at 4.) He also provided the company's "Information Systems: software policy." In general, the policy provides a list of approved software and hardware that is allowed on the company systems. An employee is encouraged to contact the help desk so that hardware or software can be evaluated and possibly approved. However, the policy also says the following:

> It is *expected* that our engineering staff will at times obtain, load, and execute software from sources outside [the company's] IS department. It is also *expected* that employees obtaining software in this manner will be sufficiently diligent and ensure that their actions do not negatively impact our computing environment from a security, availability, or interoperability aspect.
>
> It is also *expected* that our engineering staff will at times obtain hardware, install it and use it. Again diligence is required on their part to ensure that those actions do not negatively impact our computing environment. (Applicant Exhibit A at 5-7.) (Emphasis supplied.)

Specifically, Applicant was facing a time crunch on a particular project at work. He stated:

> I needed those files [for the project] quickly, and so I decided that since I had seen other people using personal devices that it would permissible, in this case, in the interest of efficiency, as long as I took appropriate precautions.
>
> So I bought a sealed thumb drive from a reputable dealer, I did not use it on any home systems. It is a personal device owned by me, but at the time I plugged it in to [sic] work systems it had never been plugged into any of my home systems. (Tr. 22.)

Applicant's supervisor at the time of the incident testified and confirmed Applicant's version of this event, and also stated that Applicant had told him of the incident at the time it occurred. He also stated, "I informed him [Applicant] that

engineers were not subject to the policy of moving files based off of thumb drives and personal devices." (Tr. 42-47.)

Mitigation

Concerning Applicant's work performance his former supervisor testified, "[Applicant] is one of our more stellar employees. I know that when his review came up I gave him high praise. I got him a promotion, I got him a raise. He's been a huge asset to the team and I haven't seen any negative feedback as far as his character or his performance." (Tr. 43.)

Applicant's current supervisor also testified. The supervisor stated that Applicant is very ethical in how he proceeds with his work. (Tr. 47-50.)

Policies

Security clearance decisions are not made in a vacuum. When evaluating an applicant's suitability for a security clearance, the administrative judge must consider the adjudicative guidelines (AG). In addition to brief introductory explanations for each guideline, the adjudicative guidelines list potentially disqualifying conditions and mitigating conditions, which are to be used as appropriate 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, these guidelines are applied in conjunction with the factors listed in AG ¶ 2 describing the adjudicative process. The administrative judge's over-arching 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. In addition, the administrative judge may also rely on his or her own common sense, as well as knowledge of the law, human nature, and the ways of the world, in making a reasoned decision.

The protection of the national security is the paramount consideration. AG ¶ 2(b) requires that, "Any doubt concerning personnel being considered for access to classified information will be resolved in favor of national security." 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.

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, and has the ultimate burden of persuasion as to obtaining a favorable clearance 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. Security clearance decisions include, by necessity, consideration of the possible risk that 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.

Finally, as emphasized in Section 7 of Executive Order 10865, "Any determination under this order adverse to an applicant shall be a determination 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

Paragraph 1 (Guideline M, Use of Information Technology Systems)

The security concern relating to 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.

Turning first to allegation 1.a. The guideline notes several conditions that could possibly raise security concerns concerning Applicant's conduct. Under AG ¶ 40(a), "illegal or unauthorized entry into any information technology system or component thereof" is potentially disqualifying. Similarly under AG ¶ 40(c), "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. However, they do not apply to Applicant's conduct. The evidence shows that Applicant was authorized by his college instructor to take the actions he took, as set forth at length in the evidence. This was in furtherance of the instructor helping a government entity investigate a computer security incident. When Applicant became concerned that there might be legal ramifications to his conduct, he stopped and appropriately approached his instructor for advice and guidance. This allegation is found for Applicant.

Turning next to allegation 1.b. Applicant admitted using a personal thumb drive on his work computer. Applicant is an engineer at his company, and as shown above is exempt from corporate policy that prohibits the introduction of outside hardware or software without permission. Accordingly, his conduct does not come under the strictures of AG ¶ 40(f), "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 and regulations*." (Emphasis supplied.) Allegation 1.b is also found for Applicant.

The guideline also includes examples of conditions that could mitigate security concerns arising from use of information technology systems. As stated, I find that Applicant's conduct is not cognizable under any of the disqualifying conditions. Assuming for the sake of argument that his conduct is cognizable, the evidence shows that all of the mitigating conditions under this guideline apply to Applicant as well. Under AG ¶ 41(a), disqualifying conditions may be mitigated where "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." In addition, AG ¶ 41(b) states that disqualifying conditions may be mitigated where "the 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." Finally, AG ¶ 41(c) states the disqualifying conditions may be mitigated where "the conduct was unintentional or inadvertent and was followed by a prompt, good-faith effort to correct the situation and by notification of supervisor."

Since I find for Applicant under Paragraph 1 because his conduct was not cognizable under the disqualifying conditions, I need not discuss his conduct under Guideline E, Personal Conduct. His actions did not involve questionable judgment, lack of candor, dishonesty, or an unwillingness to comply with rules and regulations; nor did they raise questions about his reliability, trustworthiness, or ability to protect classified information.

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 relevant circumstances. 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. The administrative judge must 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.

I considered the potentially disqualifying and mitigating conditions in light of all the relevant facts and circumstances surrounding this case. The discussion under Guidelines M and E, above, applies here as well. Applicant provided evidence showing that his conduct in both situations was appropriate and authorized. He also provided evidence showing he is quite knowledgeable about his security responsibilities and able to fulfill them. (Tr. 37-40.) Under AG ¶ 2(a)(2), I have considered the facts of Applicant's conduct. I find that there is little to no potential for pressure, coercion, exploitation, or duress (AG ¶ 2(a)(8)).

Overall, the record evidence leaves me with no questions or doubts as to Applicant's eligibility and suitability for a security clearance. For all these reasons, I conclude Applicant has mitigated the security concerns allegedly arising from his use of information technology systems and personal conduct. Accordingly, the evidence supports granting his request for a security clearance.

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

WILFORD H. ROSS
Administrative Judge