DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 16-00779
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Mary Margaret Foreman, Esq., Department Counsel
For Applicant: *Pro se*

10/26/2017

Decision

COACHER, Robert E., Administrative Judge:

The Government produced insufficient evidence to establish the alleged disqualifying conditions, or in the alternative, Applicant mitigated the Government's security concerns under Guideline M, use of information technology, and Guideline E, personal conduct. Applicant's eligibility for a security clearance is granted.

Statement of the Case

On August 3, 2016, the Department of Defense Consolidated Adjudications Facility (DOD CAF) issued Applicant a Statement of Reasons (SOR) detailing security concerns under Guideline M and Guideline E. DOD CAF acted under Executive Order (EO) 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).[1]

Applicant answered the SOR on April 7, 2015, and requested a hearing. The case was assigned to me on January 18, 2017. The Defense Office of Hearings and Appeals (DOHA) issued a notice of hearing on January 18, 2017, and the hearing was convened as scheduled on February 22, 2017. The Government offered exhibits (GE) 1 through 3, which were admitted into evidence.[2] The Government's exhibit list was marked as a hearing exhibit (HE I). Applicant testified, but did not offer documentary evidence. DOHA received the hearing transcript (Tr.) on April 19, 2017.

Findings of Fact

In Applicant's answer (Answer), he admitted in part and denied in part the allegations in the SOR. After a thorough and careful review of all the pleadings and evidence, I make the following findings of fact.

Applicant is 42 years old. He is single, never married, and has no children. He has worked for a federal contractor since 2010. He served from 2003 to 2009 in the Air Force, both active duty and in the reserve. He received an honorable discharge. He has two associate' degrees, a bachelor's degree, and a master's degree.[3]

The allegations raised in the SOR include: (1) From 1992 to 2010, Applicant illegally downloaded computer software applications, programs, and movies for his own personal use without authorization (*See* SOR ¶ 1.a); (2) Applicant illegally gained access to computer applications by using serial numbers, key codes, or other illegal means in his place of employment without authorization (*See* SOR ¶ 1.b); (3) Applicant removed information technology (IT) hardware from his employer without authorization (*See* SOR ¶ 1.c). The same allegations were also cross-alleged as personal conduct concerns (*See* SOR ¶ 2.a).

Applicant has worked with IT issues since he was 17 years old. From 1992 to 1996, he started his own bulletin board service (BBS) to share game-playing and messaging with other users. This was a time before the public internet was available. Shareware programs were uploaded to his BBS from other BBS. The purpose of

[1] I decided this case using the AG implemented by DOD on June 8, 2017. However, I also considered this case under the previous AG implemented on September 1, 2006, and my conclusions are the same using either set of AG.

[2] Applicant noted a number of inaccurate statements in GE 2 and made several verbal corrections to the document. He also objected to the admission of GE 3 because the interviewer mischaracterized his answers regarding his use of software as illegal. I overruled the objection, but advised Applicant that I would consider the weight of this evidence when viewed as a whole with the rest of the evidence in this case. Tr. 20-27, 30-31; GE 2-3.

[3] Tr. 6; GE 1.

shareware was to share these programs with other users. He followed the shareware user agreements when he either uploaded or downloaded these shareware programs. During Applicant's June 2011 interview with another government agency (AGA), the interviewer claimed Applicant stated he downloaded programs from a website. In his Answer, Applicant explained that this was impossible then because the public internet (from which one would have to download) was not in existence. Applicant believes the interviewer did not fully understand the process Applicant was describing and therefore characterized actions as "illegal," which were not necessarily so. After hearing Applicant's testimony and reviewing both summarized statements that he made to investigators (GE 2, dated December 2015 and GE 3, made to AGA in July 2011), I find that his testimony is credible and more reliable than the July 2011 summarized statement and will give it more weight (the Government did not call a witness to explain the context of the summarized interview). His testimony is also more consistent with his December 2015 summarized statement and his Answer.[4]

From 1997 to 2001, Applicant denied downloading any software programs, although he did download drivers and networking tools. The Government presented insufficient evidence of illegal downloading during this timeframe. From 2001 to 2002, Applicant admitted downloading a software program on his personal computer that was given to him by a friend. In 2003, he deployed for the Air Force. He was a system administrator in his deployed capacity. He admitted installing several software programs on his Air Force computer. Some of these programs required activation keys. These programs were used to support mission requirements. He did not specifically request permission to install these programs, but believed he had the inherent authority to do so to insure mission success. He also had access to a "morale" computer while deployed. It was used by deployed troops to play games and watch movies. He did not download any movies on to this computer. Applicant was awarded an achievement medal for his contributions to the overall mission during this deployment.[5]

From 2005 to 2006, while working as a system engineer for a health care employer, he used his personal laptop computer to support his work efforts. He legally purchased hardware with his own funds. This allowed him access to software and firmware from vendor's websites. In March 2006, during a critical system outage at work, while troubleshooting the problem, Applicant admitted using a software key (a string of characters) on a vendor's website. He believed he was authorized to use the key on a vendor website to support official company work, which is what he did in this case.[6]

From 2003 to 2006, while pursuing his bachelor's degree, he downloaded software through his college. He obtained this software either through his own

[4] Tr. 33-35; Answer; GE 2, 3.

[5] Tr. 37-38, 57-59; Answer (Answer Exh. A).

[6] Tr.40, 42; Answer.

subscription, or from a friend's subscription. This software is also available directly from the vendor. In 2010, Applicant admitted downloading a program (server) using peer-to-peer file sharing. He used this program during its trial period, meaning that the vendor allowed use of the programs for a limited period for free. He only used the program during this trial or evaluation period. The Government failed to establish what actions of Applicant were "illegal" and what the basis of the illegality was (statute, rule, regulation, company policy, etc.). Applicant was never disciplined or questioned about his software usage by any employer. He has had no issues regarding the legitimacy of his downloading of software since 2010.[7]

When Applicant left his employer in June 2010 (on good terms), he took two hard drive trays, which were discarded by his employer. These trays were not computer media of any type. They were used to hold and store hard drives. Once the hard drives were out of the trays, the trays served no purpose. Applicant realizes that he should have asked permission before he took the trays. He sent the trays back to his former employer and they were scrapped.[8]

Applicant produced five letters of recommendation from former supervisors and coworkers. Some worked with him in a classified environment. All have high regard for Applicant's IT abilities and professionalism. They support granting his clearance.[9]

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 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, 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. According to AG ¶ 2(a), the entire process is a careful weighing 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 national security

[7] Tr. 40, 81; Answer.

[8] Tr. 45-48; Answer, Answer (Exh. D-E).

[9] Answer (Exh. F).

eligibility will be resolved in favor of the 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.

Under Directive ¶ E3.1.14, the Government must present evidence to establish controverted facts alleged in the SOR. Under Directive ¶ E3.1.15, an "applicant is responsible for presenting witnesses and other evidence to rebut, explain, extenuate, or mitigate facts admitted by applicant or proven by Department Counsel, and 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 that an applicant may deliberately or inadvertently fail to safeguard classified information. Such decisions entail a certain degree of legally permissible extrapolation about potential, rather than actual, risk of compromise of classified information.

Section 7 of EO 10865 provides that 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

AG ¶ 39 expresses the security concern pertaining to use of information technology systems:

> Failure to comply 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 includes any computer-based, mobile, or wireless device used to create, store, access, process, manipulate, protect, or move information. This includes any component, whether integrated into a larger system or not, such as hardware, software, or firmware, used to enable or facilitate these operations.

AG ¶ 40 describes conditions that could raise a security concern and may be disqualifying. I have considered the following as potentially relevant:

(d) downloading, storing, or transmitting classified, sensitive, proprietary, or other protected information on or to any unauthorized information technology system; and

(e) unauthorized use of any information technology system.

The Government presented insufficient evidence to establish that Applicant's actions meet either of these disqualifying conditions. I also considered the overall concern expressed in Guideline M, and found the evidence wanting. No evidence was produced that any of Applicant's downloading or use of keys violated any law or was against any company policy. The hard drive trays were not an information technology system. Based on the record evidence, none of the above disqualifying conditions apply.

Even though I found none of the disqualifying conditions applicable, I also reviewed all of the mitigating conditions under AG ¶ 41, and I considered the following relevant:

(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 actions can be considered remote since the last alleged concern occurred in 2010. He has not experienced another issue concerning information technology systems since that time. On the contrary, his supervisors vouched for his professionalism. He provided persuasive evidence to show that sufficient time has passed since the incidents, that any security issues are unlikely to recur, and that his current reliability, trustworthiness, and good judgment are not in doubt. AG ¶ 41(a) applies.

Guideline E, Personal Conduct

AG ¶ 15 expresses the personal conduct 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 or sensitive information. Of special interest is any failure to cooperate or provide truthful and candid answers during national security investigative or adjudicative processes.

AG ¶ 16 describes conditions that could raise a security concern and may be disqualifying in this case. The following disqualifying condition is potentially applicable:

(d) credible adverse information that is not explicitly covered under any other guideline and may not be sufficient by itself for an adverse determination, but which, when combined with all available information 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. This includes but is not limited to consideration of:

(1) untrustworthy or unreliable behavior to include breach of client confidentiality, release of proprietary information, unauthorized release of sensitive corporate or other government protected information:

(2) disruptive, violent, or other inappropriate behavior in the workplace;

(3) a pattern of dishonesty or rule violations; and

(4) evidence of significant misuse of Government or other employer's time or resources.

The evidence supports that Applicant performed his duties to keep his employers' IT systems working. He did nothing for personal gain and was awarded by the Air Force for his performance. Applicant's taking of two hard drive trays of *de minimus* value, and which were ultimately scrapped, is not a significant misuse of an employer's resources. Insufficient evidence exists to establish this disqualifying condition or the overall concern stated in Guideline E.

However, I also reviewed conditions that could mitigate security concerns arising from personal conduct. I have considered all of the mitigating conditions under AG ¶ 17 and found the following relevant:

(c) 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.

Given the nature of Applicant's IT work, if any software programs were inadvertently downloaded the last action occurred seven years ago. Sufficient time has passed to attenuate Applicant's actions. I am convinced Applicant has learned from this experience and that he will be alert to prevent any recurrence. His fellow IT professionals corroborate his current reliability. AG ¶ 17(c) applies.

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(d):

> (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.

I considered the potentially disqualifying and mitigating conditions in light of all the facts and circumstances surrounding this case. I considered Applicant's military service, including his deployment and his achievement medal, the recommendations from his supervisors and coworkers, and the nature of his IT work. Even though the Government failed to establish disqualifying conditions, Applicant provided sufficient evidence to mitigate the overall security concerns raised by the allegations.

Overall, the record evidence leaves me without questions or doubts about Applicant's eligibility and suitability for a security clearance. For all these reasons, I conclude the Government's evidence was insufficient to establish the alleged security concerns, and alternatively, Applicant mitigated the security concerns arising under the Guidelines.

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 – 1.c:	For Applicant
Paragraph 1, 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.

_____

Robert E. Coacher
Administrative Judge