DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 14-01226
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Robert J. Kilmartin, Esq., Department Counsel
For Applicant: Ronald C. Sykstus, Esq.

12/01/2014

Decision

LOUGHRAN, Edward W., Administrative Judge:

Applicant mitigated the handling protected information and use of information technology systems security concerns. Eligibility for access to classified information is granted.

Statement of the Case

On July 9, 2014, the Department of Defense (DOD) issued a Statement of Reasons (SOR) to Applicant detailing security concerns under Guidelines K (handling protected information) and M (use of information technology systems). The action was taken under Executive Order (EO) 10865, *Safeguarding Classified Information within Industry* (February 20, 1960), as amended; DOD Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (January 2, 1992), as amended (Directive); and the adjudicative guidelines (AG) implemented by the DOD on September 1, 2006.

Applicant responded to the SOR on July 29, 2014, and requested a hearing before an administrative judge. The case was assigned to me on September 23, 2014. The Defense Office of Hearings and Appeals (DOHA) issued a notice of hearing on

September 29, 2014, scheduling the hearing for October 21, 2014. The hearing was convened on October 21, 2014, and reconvened on October 23, 2014. DOHA received the hearing transcript (Tr.) on October 30, 2014.

Procedural and Evidentiary Rulings

Procedure

A joint hearing was conducted for Applicant and his son. I have one set of exhibits and one transcript, but I am issuing separate decisions.

Evidence

Department Counsel called three witnesses and submitted Government Exhibits (GE) 1 through 33, which were admitted in evidence without objection. Applicant and his son testified. They called 12 additional witnesses and submitted Applicant's Exhibits (AE) A through W and AA through QQ, which were admitted without objection. Department Counsel sent an informational letter to Applicant's attorney on August 29, 2014. The letter is included in the record as Hearing Exhibit (HE) I.

Findings of Fact

Applicant is a 61-year-old employee of a defense contractor. He has worked for his current employer since 2009. He is on unpaid furlough pending the outcome of this case. He seeks to retain his security clearance, which he has held since about 2009. He has a bachelor's degree. He is married with three adult children.[1]

On a Friday in January 2012, Applicant inserted unclassified read-only compact discs (CDs) in a classified computer. Any media placed in a classified system takes on the classification of the system. He was authorized to place them in the classified computer, but the CDs became classified. Applicant inadvertently brought the now-classified CDs home, where they remained in his backpack until he returned to work the following Monday.[2]

During the weekend, the discs could not be located by the security manager. On Monday, the security manager asked Applicant about the missing discs. He produced them from his backpack. It was determined that there was no compromise or spillage. The security manager testified that Applicant was "quite contrite . . . forthright and honest about what he did." Applicant was directed to reread the security briefing and the system security plan.[3]

[1] Tr. at 46-48, 53-54, 84, 136-137; GE 14.

[2] Tr. at 66-74, 99-101, 398-399; Applicant's response to SOR; GE 13, 14, 16-18.

[3] Tr. at 73-75, 109-110, 398-399, 409-410; Applicant's response to SOR;GE 13, 14, 16-18.

Applicant and his son work for the same company. They were required to periodically spend time at an isolated location in the United States. The closest hotel to the location was more than 60 miles away. Conditions at the location were austere with few amenities. The location had a bank of classified computers that were connected to a classified network.[4]

During a trip to the isolated location in 2011, it was noted that the computers would occasionally be locked. The locked computers were being used by remote logins from other locations. Authorization was required to do remote logins. In early 2012, a secure network was created between Applicant's home location and the isolated location. Classified information could be transmitted over the secure network, and it was possible to conduct a remote login between the two locations. However, no authorization was granted to anyone at Applicant's home location to perform a remote login to the computers at the isolated location.[5]

Applicant's son traveled to the isolated location in April 2012. Applicant was unable to make the trip because of a medical condition. Applicant's son created a text file with the Internet Protocol (IP) address of the computer at the isolated location and placed the text file on the secure network. The son called Applicant and asked him to attempt a remote login from the classified computer at the home location to a classified computer at the isolated location. Applicant was authorized to log into the computers at both locations, but he never received authorization to conduct remote logins. Applicant took his son's request without question, and he did not investigate whether he was authorized to conduct a remote login to the computer at the isolated location. Applicant used the IP address that was on the text file, and he attempted a remote login to the computer at the isolated location. He was able to get to the login prompt on the screen, but he was unable to log in.[6]

The Defense Security Service (DSS) suspended Applicant's security clearance in December 2012 pending the outcome of this case. Applicant has been on unpaid furlough from his company for almost two years. He is appropriately remorseful for his actions.[7]

Numerous witnesses testified on Applicant's behalf. He also submitted a large amount of documents and letters. Applicant is praised for his excellent job performance, as well as his honesty, dedication, reliability, trustworthiness, and integrity.[8]

[4] Tr. at 57-63, 146-148; GE 4, 5, 23.

[5] Tr. at 63-64, 77-78, 105, 134, 150, 208-211; Applicant's response to SOR; GE 4, 5, 10, 23.

[6] Tr. at 59-60, 77-84, 102, 106, 110, 119-120, 163-164, 207, 222-223, 273; Applicant's response to SOR; GE 4, 5, 10, 17, 19, 20, 23.

[7] Tr. at 136-137; Applicant's response to SOR; GE 33.

[8] AE A-V.

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."

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 K, Handling Protected Information

The security concern for handling protected information is set out in AG ¶ 33:

> Deliberate or negligent failure to comply with rules and regulations for protecting classified or other sensitive information raises doubt about an individual's trustworthiness, judgment, reliability, or willingness and ability to safeguard such information, and is a serious security concern.

AG ¶ 34 describes conditions that could raise a security concern and may be disqualifying. The following are potentially applicable:

> (b) collecting or storing classified or other protected information at home or in any other unauthorized location;
>
> (d) inappropriate efforts to obtain or view classified or other protected information outside one's need to know; and
>
> (g) any failure to comply with rules for the protection of classified or other sensitive information.

Applicant took classified discs home. He attempted a remote login to a classified computer when he was not authorized to do so. The evidence raises the above disqualifying conditions.

Conditions that could mitigate handling protected information security concerns are provided under AG ¶ 35. The following are potentially applicable:

> (a) so much time has elapsed since the behavior, or it has happened so infrequently or under such unusual circumstances, that it is unlikely to recur and does not cast doubt on the individual's current reliability, trustworthiness, or good judgment; and
>
> (b) the individual responded favorably to counseling or remedial security training and now demonstrates a positive attitude toward the discharge of security responsibilities.

The first incident was an honest mistake that could have happened to almost anyone. However, it put Applicant on notice, and he should have exercised more care during the second incident. He was authorized to log into the classified computers at both locations, but he had no authorization to log in remotely. Applicant relied on his son to his own detriment. Nonetheless, I am convinced that Applicant is remorseful for his actions, he possesses a positive attitude toward the discharge of his security responsibilities, and he will not repeat the behavior. Both mitigating conditions are applicable.

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 ability to 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.

AG ¶ 40 describes conditions that could raise a security concern and may be disqualifying. The following are potentially applicable:

> (a) illegal or unauthorized entry into any information technology system or component thereof;
>
> (c) use of any information technology system to gain unauthorized access to another system or to a compartmented area within the same system; and
>
> (e) unauthorized use of a government or other information technology system.

Applicant attempted an unauthorized remote login to a classified computer. The above disqualifying conditions are applicable.

Conditions that could mitigate the use of information technology systems security concerns are provided under AG ¶ 41. The following is potentially 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.

AG ¶ 41(a) is applicable under the same rationale discussed in the analysis for handling protected 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 relevant 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.

I considered the potentially disqualifying and mitigating conditions in light of all the facts and circumstances surrounding this case. I have incorporated my comments under Guidelines K and M in my whole-person analysis. Some of the factors in AG ¶ 2(a) were addressed under those guidelines, but some warrant additional comment.

I considered Applicant's excellent character evidence. He was involved in two security violations. One was inadvertent, and the inappropriate actions of his son significantly contributed to the second. Security violations are one of the strongest possible reasons for denying or revoking access to classified information, as they raise serious questions about an applicant's suitability for access to classified information. Once it is established that an applicant has committed a security violation, he has a very heavy burden of demonstrating that he should be entrusted with classified information. Because security violations strike at the very heart of the industrial security program, an administrative judge must give any claims of reform and rehabilitation strict scrutiny. In many security clearance cases, applicants are denied a clearance for having an indicator of a risk that they might commit a security violation (e.g., alcohol abuse, delinquent debts, or drug use). Security violation cases reveal more than simply an indicator of risk.[9] The frequency and duration of the security violations are also aggravating factors.[10]

Applicant is remorseful for his conduct. I further believe the experience of going through the adjudicative process had an additional value, in that Applicant is cognizant that he must be more diligent in his responsibilities for safeguarding classified information. He has met his heavy burden of demonstrating that it is clearly consistent with the national interest to continue his security clearance.

Overall, the record evidence leaves me without questions or doubts as to Applicant's eligibility and suitability for a security clearance. I conclude Applicant mitigated the handling protected information and use of information technology systems security concerns.

[9] ISCR Case No. 03-26888 (App. Bd. Oct. 5, 2006).

[10] ISCR Case No. 97-0435 at 5 (App. Bd. July 14, 1998).

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 K:	For Applicant
Subparagraphs 1.a-1.b:	For Applicant
Paragraph 2, Guideline M:	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 continue Applicant's eligibility for a security clearance. Eligibility for access to classified information is granted.

_____
Edward W. Loughran
Administrative Judge