DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 14-02447
	)	
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 did not mitigate the personal conduct, handling protected information, and use of information technology systems security concerns. Eligibility for access to classified information is denied.

Statement of the Case

On July 2, 2014, the Department of Defense (DOD) issued a Statement of Reasons (SOR) to Applicant detailing security concerns under Guidelines E (personal conduct), 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 28, 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 father. 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 father 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.

Motion to Amend SOR

Department Counsel moved to amend SOR ¶ 1.b by changing the date "August 2012" to "April 2012." The motion was granted over Applicant's objection.[1]

Findings of Fact

Applicant is a 34-year-old employee of a defense contractor. He has worked for his current employer since 2002. He seeks to retain his security clearance, which he has held since about 2002. He has a bachelor's degree. He is married with three minor children.[2]

Applicant and his father 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.[3]

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. The approved way

[1] Tr. at 422-426.

[2] Tr. at 194-197; GE 1.

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

to conduct remote logins was through Remote Desktop.[4] 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 traveled to the isolated location in April 2012. His father was unable to make the trip because of a medical condition. Applicant 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. He called his father and asked him to attempt a remote login from the classified computer at the home location to a classified computer at the isolated location using Remote Desktop. His father was able to use 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. Applicant's father indicated that he thought the date of the attempted remote login was April 26, 2012.[6]

Applicant created a Secure Shell (SSH)[7] key while he was at the isolated location. He used the SSH key to create a connection between the computers at the isolated location and the home location. This was in essence a remote login, but through a different means than the approved way for remote logins, which is Remote Desktop. Applicant did not seek authorization from the home location to do a remote login or to use the SSH key. The SSH key created a connection between the two computers that remained open. Installing and using the SSH key to create a remote login was prohibited.[8]

The information system security manager for the classified program (Mr. A) worked from the home location, but he also spent time at the isolated location. In May 2012, he was notified of a problem at the isolated location. He had the system

[4] **Remote Desktop Connection** is a Microsoft Windows-based product that permits the user to connect to a computer running Windows from another computer running Windows that is connected to the same network or the Internet. *See* http://windows.microsoft.com/en-us/windows/connect-using-remote-desktop-connection#connect-using-remote-desktop-connection=windows-7.

[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, 77-82, 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] **Secure Shell** (**SSH**) is a cryptographic network protocol for secure data communication, remote command-line login, remote command execution, and other secure network services between two networked computers. It connects, via a secure channel over an insecure network, a server and a client running SSH server and SSH client programs, respectively. The encryption used by SSH is intended to provide confidentiality and integrity of data over an unsecured network, such as the Internet. SSH is typically used to log into a remote machine and execute commands. *See* http://en.wikipedia.org/wiki/Secure_Shell.

[8] Tr. at 236-242, 267-268, 277, 316-321, 357-363, 443-445, 464-466, 473-477; Applicant's response to SOR; GE 5, 10.

administrator at the home location (Ms. B) monitor the system. On June 7, 2012, Ms. B conducted a maintenance check on the network. She discovered a folder that was used by Applicant and his father. The folder contained the text file with the IP addresses and a shortcut to Remote Desktop.[9]

Applicant discussed his father's attempted remote login in an e-mail dated June 8, 2012. The SSH key had not been discovered yet, nor was it known that Applicant connected from the isolated-location computer to the home-location computer using the SSH key. Applicant never discussed the SSH key.[10] He wrote:

> To my knowledge, [Applicant's father] only attempted the login on that day in April. I myself only tried "remote" logins between computers at [isolated location] based on information from System Administrators. I have not attempted a remote login from the [home location] to [isolated location].[11]

In August 2012, Mr. A and Ms. B traveled to the isolated location. While there, a system administrator at the site (Mr. C) discovered the BIOS (Basic Input/Output System) setting on two computers had been changed. The modification permitted a connection between computers using an SSH key. After they returned to the home location, Ms. B discovered the SSH key on a computer used by Applicant and his father.[12]

The security manager at the home location (Ms. D) testified that installing any unauthorized software on the computer system was in direct violation of the user agreement signed by Applicant. Use of an SSH key was not permitted. She also testified that Applicant did not have authorization to conduct a remote login from the isolated location to the home location.[13]

Applicant has consistently maintained that he had authorization to conduct a remote login. He stated that on his April 2012 trip to the isolated location, he attempted a remote login from one computer to another computer at the isolated location. He was unsuccessful. He stated that he went to one of the system administrators (Ms. E) who told him that he would have to be added to the correct group. He testified that she added him to the group and told him that he was authorized to conduct a remote login from the isolated location to the home location. He asked her if it was possible to conduct a remote login from the home location to the isolated location. She told him that

[9] Tr. at 440-445; GE 10, 20.

[10] GE 23.

[11] GE 23.

[12] Tr. at 400-401, 407-408, 440-445, 455-462, 475-477; GE 10, 11, 25.

[13] Tr. at 400-401, 407-408; AE OO.

it was possible, and that if there were any problems, he should let her know. He then remotely logged in from one computer to another computer at the isolated location.[14]

Applicant admitted that he created a text file with the computer's IP address, and he called his father and asked him to do a remote login to the isolated-location computer from the home-location computer. He stated that he did not expect his father to be able to remotely log in, but he wanted to see if the prompt came up so that he could do a remote login when he returned to the home location. Applicant never attempted a remote login from the home location. He stated that there was no need for a remote login before it was discovered in June 2012.[15]

Applicant admitted that he created the SSH key and conducted a remote login from the isolated location to the home location. He stated that he did not seek permission because he thought he only needed permission to conduct a remote login using Remote Desktop, and that he did not need permission to do so using the SSH key. He stated that he had authorization to conduct the remote login using Remote Desktop, but he created the SSH key "to enable easier access." He denied modifying the BIOS on any computers at the isolated location.[16]

Ms. E testified that she did not grant Applicant permission to conduct a remote login. Requests to conduct remote logins had to be submitted via a form to the security team to approve the request. Ms. E would not add anyone to the group that was authorized to conduct remote logins unless she was directed to do so by the security team. She indicated that there were two user groups: one user group could remotely access one computer at the isolated location to another computer at that location. The second group was authorized to remotely log in from another location to the isolated location using Remote Desktop. If someone wanted remote access from the isolated location to the home location, the person would have to seek authorization from the home location. Using an SSH key to remotely log in to or from the isolated location was not permitted.[17]

Ms. E left her position at the isolated location in March 2012 to take another job. The job did not work out, and she returned to work at the isolated location on April 26, 2012, a Thursday. She did not have full access on April 26, 2012, and had to be escorted at the site. She did not gain full access until the following week. The computer system at the isolated location has been disassembled, and Ms. E no longer works there. She does not remember Applicant or his father by name. She has not seen them since before she was asked about them in June 2012. She stated that she might

[14] Tr. at 212-217, 230-234, 255-257; Applicant's response to SOR; GE 4, 5, 23.

[15] Tr. at 215-230, 275; Applicant's response to SOR; GE 4, 5.

[16] Tr. at 357-363, 462, 507-508; Applicant's response to SOR; GE 5.

[17] Tr. at 370-392; AE OO-QQ.

recognize them if she saw their faces, but she testified telephonically and never had the chance to identify them.[18]

Applicant provided an affidavit to an Office of Personnel Management (OPM) investigator in December 2012. He stated that he asked Ms. E for remote access, and she added him to the remote-access user group. He admitted asking his father to attempt a remote login from the home location. He also admitted creating and using the SSH key to log in from the isolated location to the home location, but he stated that he "believed using SSH as a non-administrator was allowable."[19]

Applicant provided another affidavit to an OPM investigator in June 2013. He stated that he asked Ms. E how his father could remotely log in from the home location. He stated that she added him to the remote-access user group. He asked his father to attempt a remote login from the home location. He also admitted creating and using the SSH key in April 2012. He denied attempting any remote logins after April 2012.[20]

Applicant's facility security officer (FSO) directed Applicant to take remedial security training after the incidents. The FSO indicated that the matter was a "he said, she said" issue between Applicant and Ms. E, and that there was "no documented proof that a violation occurred." The Defense Security Service (DSS) suspended Applicant's security clearance in November 2012 pending the outcome of this case.[21] Applicant has been retained by his company, and he is working on non-classified projects pending the outcome of this case.[22]

Applicant called numerous witnesses and submitted documents and letters attesting to his outstanding job performance, character, honor, professionalism, sincerity, trustworthiness, honesty, loyalty, reliability, dedication, and integrity. He is active in his community. He is enthusiastically recommended for a security clearance.[23]

I considered the possibility that this case resulted from an honest mistake or misunderstanding. However, those possibilities are rejected. I did not find Applicant credible. He did not satisfactorily explain why he needed to create an SSH key to conduct a remote login if he had authorization to conduct logins using the approved Remote Desktop means. Ms. E did not recognize Applicant's or his father's name, but she did not have the opportunity to see either of them and might have recognized them if she had. I also considered the testimony that she could not have granted Applicant

[18] Tr. at 392-393, 468-472, 482; GE 10.

[19] GE 4.

[20] GE 5.

[21] I have made an independent evaluation of the evidence, and I have not relied on the FSO's opinion or the fact that DSS suspended Applicant's security clearance in arriving at my decision.

[22] GE 9; AE W, PP.

[23] AE AA-NN.

permission because she had just returned to work on April 26, 2012, she had to be escorted, and she did not have full access until the following week. I find Applicant's failure to mention the SSH key and his remote login in his June 2012 e-mail to be misleading.

After considering all the evidence, I do not find that Applicant sought or obtained approval from Ms. E to conduct remote logins. I further find that Applicant intentionally provided false information in his December 2012 and June 2013 affidavits when he stated that he had authorization from Ms. E to conduct remote logins.

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 E, Personal Conduct

The security concern for personal conduct is set out in AG ¶ 15, as follows:

> 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.

AG ¶ 16 describes conditions that could raise a security concern and may be disqualifying. The following disqualifying conditions are potentially applicable:

> (b) deliberately providing false or misleading information concerning relevant facts to an employer, investigator, security official, competent medical authority, or other official government representative; and
>
> (e) personal conduct, or concealment of information about one's conduct, that creates a vulnerability to exploitation, manipulation, or duress, such as . . . engaging in activities which, if known, may affect the person's personal, professional, or community standing.

Applicant asked his father to attempt a remote login from the classified computer at the home location to a classified computer at the isolated location. Applicant created an SSH key and conducted a login from the isolated location to the home location. None of these actions were authorized. That conduct created a vulnerability to exploitation, manipulation, and duress. AG ¶ 16(e) is applicable. Additionally, the conduct showed poor judgment and an unwillingness to comply with rules and regulations, which raises questions about Applicant's ability to protect classified information. The general concern addressed in AG ¶ 15 is also raised. *See* ISCR Case No. 12-01683 at 4 (App. Bd. Jun. 10, 2014).

Applicant intentionally provided false information in his December 2012 and June 2013 affidavits when he stated that he had authorization from Ms. E to conduct remote logins. AG ¶ 16(b) is applicable.

The evidence does not support a finding that Applicant attempted to use the SSH key to attempt a remote login in August 2012. SOR ¶ 3.d is concluded for Applicant.

AG ¶ 17 provides conditions that could mitigate security concerns. The following are potentially applicable:

> (a) the individual made prompt, good-faith efforts to correct the omission, concealment, or falsification before being confronted with the facts;
>
> (b) the refusal or failure to cooperate, omission, or concealment was caused or significantly contributed to by improper or inadequate advice of authorized personnel or legal counsel advising or instructing the individual specifically concerning the security clearance process. Upon being made aware of the requirement to cooperate or provide the information, the individual cooperated fully and truthfully;
>
> (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;
>
> (d) the individual has acknowledged the behavior and obtained counseling to change the behavior or taken other positive steps to alleviate the stressors, circumstances, or factors that caused untrustworthy, unreliable, or other inappropriate behavior, and such behavior is unlikely to recur;
>
> (e) the individual has taken positive steps to reduce or eliminate vulnerability to exploitation, manipulation, or duress; and
>
> (f) the information was unsubstantiated or from a source of questionable reliability.

Applicant has not accepted responsibility for his conduct. I found him less than completely forthcoming at the hearing. Without complete candor, I am unable to find that Applicant has learned from the experience and such behavior is unlikely to recur. No mitigating conditions apply.

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;
>
> (b) illegal or unauthorized modification, destruction, manipulation or denial of access to information, software, firmware, or hardware in an information technology system;
>
> (c) use of any information technology system to gain unauthorized access to another system or to a compartmented area within the same system;
>
> (e) unauthorized use of a government or other information technology system; and
>
> (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 or regulations.

Applicant participated in his father's attempted remote login; he created an SSH key; and he used the SSH key to conduct a remote login. All of 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 are 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; and
>
> (b) 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.

Applicant's conduct was not minor. He has not been forthcoming about his actions. His conduct continues to cast doubt on his current reliability, trustworthiness, and good judgment. There are no applicable mitigating conditions.

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 is potentially applicable:

(g) any failure to comply with rules for the protection of classified or other sensitive information.

Applicant asked his father to attempt a remote login from the classified computer at the home location to a classified computer at the isolated location. AG ¶ 34(g) is applicable. There are no applicable mitigating conditions under the same rationale discussed in the analysis for personal conduct and use of information technology systems.

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 E, 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 strong character evidence and his stable work history. However, Applicant has a problem with honesty and following rules. I have concerns about his judgment, trustworthiness, and willingness to safeguard classified information.

Overall, the record evidence leaves me with questions and doubts as to Applicant's eligibility and suitability for a security clearance. I conclude Applicant did not

mitigate the personal conduct, handling protected information, and use of information technology systems security concerns.

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:	Against Applicant
Subparagraph 1.a:	Against Applicant
Paragraph 2, Guideline M:	Against Applicant
Subparagraphs 2.a-2.b:	Against Applicant
Paragraph 3, Guideline E:	Against Applicant
Subparagraphs 3.a-3.c:	Against Applicant
Subparagraph 3.d:	For Applicant

Conclusion

In light of all of the circumstances presented by the record in this case, it is not clearly consistent with the national interest to continue Applicant's eligibility for a security clearance. Eligibility for access to classified information is denied.

_____
Edward W. Loughran
Administrative Judge