DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 15-05020
	)	
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Adrienne Driskill, Esq., Department Counsel
For Applicant: Cathryn E. Young, *Esq.*

December 15, 2017

_____

Decision

_____

MOGUL, Martin H., Administrative Judge:

Statement of the Case

On August 17, 2016, in accordance with Department of Defense (DoD) Directive 5220.6, as amended (Directive), the DoD issued Applicant a Statement of Reasons (SOR) alleging facts that raise security concerns under Guidelines J, K, and M.[1] The SOR further informed Applicant that, based on information available to the government, DoD adjudicators could not make the preliminary affirmative finding it is clearly consistent with the national interest to grant or continue Applicant's security clearance.

On October 6, 2016, Applicant submitted a written reply to the SOR (RSOR), and requested that the case be decided after a hearing before an administrative judge. The case was assigned to this administrative judge on November 29, 2016. The Defense

[1] I considered the previous Adjudicative Guidelines, effective September 1, 2006, as well as the new Adjudicative Guidelines, effective June 8, 2017. My decision would be the same if the case was considered under the previous Adjudicative Guidelines, effective September 1, 2006.

Office of Hearings and Appeals (DOHA) issued a notice of hearing on that date, scheduling the hearing for January 12, 2017. The hearing was convened as scheduled.

At the hearing, the Government offered Exhibits 1 through 4, which were admitted without objection. Applicant testified on his own behalf and presented six documents, which were also admitted without objection as Exhibits A through F. One additional witness testified on behalf of Applicant. The record was left open until January 26, 2017, for receipt of additional documentation. Documents were submitted and have been marked and entered into evidence without objection as Exhibit G. DOHA received the transcript of the hearing (TR) on January 19, 2017. Based upon a review of the pleadings, exhibits, and the testimony of Applicant and the additional witness, eligibility for access to classified information is granted.

Findings of Fact

After a thorough and careful review of the pleadings, exhibits, and testimony, I make the following findings of fact:

Applicant is 50 years old. He is unmarried, but was previously married from 1987 to 2008, and he has no children. Applicant received an Associate of Arts degree in Electronic Engineering in 1987. Applicant is employed as a Computer Systems Analyst for a defense contractor for whom he has been employed since 2004, and he seeks a DoD security clearance in connection with his employment in the defense sector. (Tr at 34-39.)

Guideline J – Criminal Conduct

At the hearing, Applicant testified that the information that is alleged in this SOR was revealed by Applicant in 2004, during an interview that was held after Applicant took a polygraph procedure. He testified that initially he did not reveal any information, but when he was confronted by the polygraph operator that there seemed to be inconsistencies, he "searched his mind for something that would be something that maybe I've done that's wrong," and he revealed some of this information. (Tr at 39-41.)

The SOR lists one allegation 1.a. regarding Criminal Conduct, under Adjudicative Guideline J.:

1.a. It is alleged in the SOR that Applicant has stolen thousands of dollar's worth of computer equipment and software from his employer since 2001, including United States Government owned items. The stolen items include a computer, camera, mouse cables, Microsoft Windows XP, etc.

Applicant admitted that in 2001, he took home a computer from a former employer that had been owned by the Federal Government. He stated that the computer he took was one that was not being used, and he believed that it was going to be sold off for a minimal amount of money. He believed that he could put it to better use than just having it sold as "scrap," so he took it home, and he eventually gave it to a

friend. He averred that the computer had always been considered an unclassified computer, and in fact, it had never been used and it was still in an unopened box. The computer box also contained the camera, mouse and some of the other equipment described in the allegation. Applicant conceded that this was a terrible idea and a big mistake, and he would never do such a thing again. (Tr at 43-49, 102-104.)

Applicant also admitted to taking home software. He stated that he took it home so he could put it on his home computer, and it would help him learn more about computers to help him do his job better. He testified that he never made extra copies of it or tried to sell it or profit from it in any way, and nothing on the software was classified or privileged. Applicant did concede that he put the software on some other people's computers, but contended that it was done so that he could see how to fix it if there were other problems. Applicant averred that he has never taken any computers, software or any other Government or company owned equipment without permission since 2001, with the exception of one mouse that he took in 2004. He vowed that he never would he never take anything again. Finally, Applicant stated that he never was criminally charged for this conduct (Tr at 50-56, 112-118.)

Guideline K – Handling Protected Information

The SOR lists four allegations, 2.a. through 2.d., regarding Criminal Conduct, under Adjudicative Guideline J.:

2.a. It is alleged in the SOR that Applicant abused his privileges as a System Administrator by accessing co-workers personal files, profiles and emails.

Applicant admitted this conduct occurred from approximately 2002 to 2004. He accessed information from his computer that was centrally stored. Applicant testified that he accessed personal information on individuals' home directories. While he conceded that he should not have done that, he averred that he had never been instructed or trained not to go into someone's home directory. He estimated that he accessed home directory information about 12 times. Finally he testified that though he has continued to have access to an individual's information on the home directory, he has never done it since 2004, when he had his first polygraph examination, and became aware that it was not something he should do. He also averred that he would not do it in the future. (Tr at 56-64.)

2.b. It is alleged in the SOR that Applicant abused his privileges as a System Administrator by deliberately viewing information including company pay scales, salaries, etc., on his employer's computer network that he had no legitimate business reason or authorization to view.

Applicant also admitted this conduct occurred on one occasion during the period from approximately 2002 to 2004. He accessed information on his company's public drive. The information that he saw was what his company was charging the Government for each company position. Applicant averred that he did not do anything

with this information. He also testified that he has never accessed this information since the one time, and he would never do it again. (Tr at 64-71.)

2.c. It is alleged in the SOR that Applicant abused his privileges as a System Administrator by copying to a disk, and bringing it home to read without authorization, a one thousand page document, which contained proprietary information.

Applicant also admitted this conduct occurred on one occasion during the period from approximately 2002 to 2003. The document referred to in this allegation was a copy of the contract that the company by whom he was employed had with the Government. He had not been searching for it, but he just came across it in the regular course of his work. He testified that the document was not classified, and he did not recall it being marked as company confidential. He explained that his reason for wanting to review the document was to see what the contract showed about his company's future regarding his work. He explained that the document had what he described as "1000's of pages of legal contract," so he never even tried to go through it. He thereafter shredded the disk containing the document. Applicant averred that he did not do anything with this information. He also testified that he has never accessed this information since the one time, and he would never do it again. (Tr at 71-76.)

2.d. It is alleged in the SOR that Applicant failed to protect his computer terminal, and therefore his System Administrator privileges, from unauthorized access when he left his computer unattended and connected to the server on numerous occasions.

Applicant admitted this conduct occurred during the period from approximately 2004 to 2011. He explained that he would log onto his computer with his regular account, and then he might have to access a remote server or computer, and there were times when he did not log out of his computer to lock the system. He discussed this during a polygraph interview in 2011, and since then he has been very conscious of this, and made sure to lock his computer every time when he leaves it. Applicant averred that he has never been cited for this behavior. (Tr at 76-80.)

Guideline M – Use of Information Technology

The SOR lists three allegations, 3.a through 3.c., regarding Use of Information Technology, which will be reviewed below:

3.a. It is alleged in the SOR that Applicant failed to adhere to Information Technology security protocol when he did not document all software and program uploads and/or installs to the United States Government computer systems.

Applicant admitted this conduct occurred during the period from approximately 2004 to 2007. He explained that this was something he was doing as a function of his job. He would download information and after scanning it for viruses, he would add it to the system to make the system work more efficiently. Applicant contended that it was never documented to him that it was part of IT protocol that he had to identify any download that was added to the computer, and he believed that other IT individuals in

his company were also downloading information without necessarily documenting the information. Applicant testified that since he became aware of the requirement that information on a classified system must be documented before he it is downloaded, he has never downloaded information onto a classified system without documenting it. Finally he testified that for the last three years, he has not worked on a classified system. (Tr at 80-85.)

3.b. It is alleged in the SOR that Applicant took United States Government and employer software and installed it on his home computer and other computers without authorization.

Applicant testified that this allegation was referring to SOR allegations 1.a. and 2.c., which occurred in approximately 2001 to 2003, and both have been reviewed above. (Tr at 85-87.)

3.c. It is alleged in the SOR that Applicant's conduct, set forth in subparagraphs 2.a. through 2.d., above, raises concern under Guideline M.

Applicant testified that he started working on classified systems in 2004 and continued until 2011, after his last polygraph, when he was removed from classified information. (Tr at 101.) During that time the security for all computer systems has gotten more serious and more involved. He has also received a number of training courses to help him understand his duties and responsibilities with the systems. Applicant credibly testified that because of his training, his experience going through the polygraph exams, and his continued experience as a computer technician, in the future he would not commit any of the conduct that was alleged in the SOR. (Tr at 140-142.)

Mitigation

As reviewed above, one additional witness testified on behalf of Applicant. The witness has known Applicant since 2003 or 2004 as a co-worker until 2013 when she retired. Within the last five years of her employment she shared a cubicle with Applicant. The witness testified that she considered Applicant to be trustworthy, reliable and displayed good judgment. (Tr at 19-32.)

Applicant also submitted a number of documents in mitigation. They included but were not limited to: four certificates of training that Applicant has received (Exhibit A); 12 extremely positive character letters (Exhibit B); and Applicant's positive performance evaluations from his present employer for 2012 to 2016. (Exhibit F.)

Policies

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 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 AG ¶ 2 describing 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 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 national security eligibility 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.

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 applies for access to classified information seeks to enter 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 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.

Section 7 of Executive Order (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 J, Criminal Conduct

The security concern relating to the guideline for Criminal Conduct is set out in AG ¶ 30:

> Criminal activity creates doubt about a person's judgment, reliability, and trustworthiness. By its very nature, it calls into question a person's ability or willingness to comply with laws, rules and regulations.

AG ¶ 31 describes conditions that could raise a security concern and may be disqualifying. The following is potentially applicable:

> (b) (evidence . . . of criminal conduct, regardless of whether the individual was formally charged, prosecuted or convicted.

Applicant did steal a computer and other items in the computer box in 2001 and a computer mouse in 2004. While the items may have been unused and headed to not be used in the future, they did not belong to Applicant and his taking of them was a criminal act. This offense gives rise to concerns about Applicant's judgment and reliability, because of the nature of the criminal offenses. The aforementioned disqualifying condition has been established.

AG ¶ 32 describes conditions that could mitigate a security concern. The following is applicable and controlling under this guideline:

> (d) there is evidence of successful rehabilitation; including but not limited to the passage of time without recurrence of criminal activity, restitution, compliance with the terms of parole or probation, job training or higher education, good employment record, or constructive community involvement.

Because Applicant's theft of the computer occurred in 2001, more than 15 years ago, I find that this Criminal Conduct mitigating condition is applicable under AG ¶ 32. Applicant's criminal past does not continue to cast doubt on his trustworthiness and judgment. I, therefore, find Guideline J for Applicant.

Guideline K, Handling Protected Information

The security concern relating to the guideline for Handling Protected Information is set out in AG ¶ 33:

> Deliberate of negligent failure to comply with rules and regulations for handling protected information - which includes classified and other sensitive government information, and proprietary information - raises doubt about an individual's trustworthiness, judgment, reliability, or willingness and ability to safeguard such information, and is a serious concern.

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

> (b) collecting or storing protected information in any unauthorized location;
>
> (c) loading, drafting, editing, . . . on any unauthorized equipment or medium;

(d) Inappropriate efforts to obtain . . . information outside one's need to know;

(f) viewing or downloading information . . .the individual's need-to-know: and

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

Applicant's history regarding protected information gives rise to concerns about Applicant's judgment and reliability. The aforementioned disqualifying condition has been established.

One mitigating condition under AG ¶ 32 is applicable:

(a) So much time has elapsed since the behavior . . . that it is unlikely to recur and does not cast doubt on the individual's current reliability, trustworthiness, or good judgment.

I considered several factors that have mitigated the Applicant's Handling Protected Information concerns. Most of Applicant's conduct that is alleged in the SOR occurred in the early 2000s more than 15 years ago, and there have been no violations since 2011, a period of more than five years. Not only did I consider Applicant's demeanor and perceived veracity in reaching my decision, I considered his overall employment history, the testimony of the character witness, and the very persuasive character letters written on his behalf.

I find that Appellant has presented evidence to show that similar conduct is unlikely to recur. I, therefore, find Guideline K Handling Protected Information for Applicant.

Guideline M, Use of Information Technology

The security concern relating to the guideline for Use of Information Technology is set out in AG ¶ 39:

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.

The guideline notes several conditions that could raise security concerns 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;
>
> (d) downloading, storing, or transmitting classified, sensitive, proprietary, or other protected information on or to any unauthorized information technology system;
>
> (e) unauthorized use of any information technology system;
>
> (f) introduction, removal, or duplication of hardware, firmware, software, or media to or from any information technology system when prohibited by rules, procedures, guidelines, or regulations or when otherwise not authorized; and
>
> (g) negligence or lax security practices in handling information technology that persists despite counseling by management.

Based on the allegations and the facts of this case concerning Applicant's past employment history, I find that AG ¶ 40 (c), (d), (e), (f), and (g) are potentially applicable in this case.

AG ¶ 41 provides conditions that could mitigate security concerns. I considered all of the mitigating conditions under AG ¶ 41 including:

> (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;

I find that AG ¶ 41(a) applies and is controlling since most of Applicant's conduct that is alleged in the SOR occurred in 2001, and there have been no violations for several years. I, therefore, find Guideline M Use of Information Technology for Applicant.

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(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 facts and circumstances surrounding this case. I have incorporated my comments under Guidelines J, K, and M in my whole-person analysis. Overall, the record evidence leaves me with no significant questions and doubts as to Applicant's eligibility and suitability for a security clearance. For all these reasons, I conclude Applicant has mitigated the security concerns under the whole-person concept.

Formal Findings

Formal findings for or against Applicant on the allegations set forth in the SOR, as required by ¶ E3.1.25 of the Directive, are:

Paragraph 1, Guideline J:	FOR APPLICANT
Subparagraph 1.a:	For Applicant
Paragraph 2, Guideline K:	FOR APPLICANT
Subparagraph 2.a:	For Applicant
Subparagraph 2.b:	For Applicant
Subparagraph 2.c:	For Applicant
Subparagraph 2.d:	For Applicant
Paragraph 3, Guideline M:	FOR APPLICANT
Subparagraph 3.a:	For Applicant
Subparagraph 3.b:	For Applicant
Subparagraph 3.c:	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.

Martin H. Mogul
Administrative Judge