DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 18-01813
	)	
Applicant for Security Clearance	)	
	)	

Appearances

For Government: Ross Hyams, Esq., Department Counsel
For Applicant: John V. Berry, Esq.
09/20/2019

_____

Decision

_____

MASON, Paul J., Administrative Judge:

Applicant's credible testimony, combined with his favorable character evidence, sufficiently dispels the security concerns arising from the guidelines for personal conduct, criminal conduct, and misuse of information technology systems. Eligibility for security clearance access is granted.

Statement of the Case

On August 24, 2017, Applicant signed and certified an Electronic Questionnaire for Investigations Processing (e-QIP) application for a security clearance. He provided a personal subject interview (PSI) on March 13, 2018. When the Department of Defense (DOD) could not make a preliminary affirmative finding required to grant a security clearance, DOD issued to Applicant a Statement of Reasons (SOR), dated August 24, 2018, detailing security concerns under the guidelines for personal conduct (Guideline E), criminal conduct (Guideline J), and misuse of technology systems (Guideline M). The action was taken under Executive Order (E.O.) 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 *National Security Adjudicative Guidelines for Determining*

Eligibility for access to Classified Information or Eligibility to Hold a Sensitive Position (AGs). On June 8, 2017, these guidelines were made applicable to all individuals who require initial or continued eligibility for access to classified information or eligibility to hold a sensitive position.

Applicant provided his notarized answer to the SOR on September 18, 2018. The case was assigned to me on January 16, 2019. The Defense Office of Hearings and Appeals (DOHA) issued a notice of hearing on February 27, 2019, for a hearing on March 18, 2019. The hearing was held as scheduled. The Government's five exhibits (GE) 1-5 and Applicant's seven exhibits (AE) A-G were entered into evidence without objection. On March 26, 2019, DOHA received the transcript (Tr.) and the record closed.

Procedural Matters

The reference to SOR "2.a" at the end of the SOR 1.b allegation (page 2) is incorrect. SOR "2.a" is amended by changing the reference to SOR "1.a" where the alleged reasons for Applicant's termination are described in greater detail. This amendment is authorized under E3.1.17 of DOD Directive 5220.6.

Findings of Fact

In his answer to the SOR, Applicant denied SOR 1.a concerning his termination from his employment after he allegedly stole a company laptop. Although he was terminated from his job on June 6, 2017, he did not steal the laptop at issue. He was authorized to carry in and take laptops (and other equipment) out of the special compartmented information facility (SCIF) and into the storage area. He was not aware of a change in corporate policy disallowing his access to the storage area. He denied SOR 1.b in part because he knew he was terminated for violating corporate policy, but did not know the specific reasons why. Applicant's denial of SOR 1.c is based on his belief he provided truthful information to the OPM investigator in the March 2018 PSI, although he was still unaware of the specific reasons for his termination. Applicant denied SOR 2.a because he did not commit a criminal offense when he used the laptop. He never attempted to steal the laptop. He denied that he failed to comply with rules applying to information technology systems as alleged under SOR 3.a. He followed policy and protocols in regularly handling laptops in the SCIF. If he had known about the new restrictive policies, he would have complied with them. (September 2018 answer to SOR)

Appellant is 58 years old. He has been married to his second wife since 1986 and has two adult-aged children. Applicant served in the United States Navy (USN) from 1978 until his honorable discharge in 1998. In 2005 and 2006, he took some courses online. Since December 2017, he has been working for a defense contractor as an information systems security manager. Before his current job, he worked for six months with another contractor, but left his position due to a reduction in job benefits. Between April 2013 and his termination in June 2017 (SOR 1.a), he was employed as a

corporate information security manager by a defense contractor. From 2005 to April 2013, Applicant was an information security manager for another contractor; his supervisor during this period was the vice president of government security who terminated Applicant in June 2017. Applicant is certified as an information system security professional. He has held a security clearance since 1978. (GE 1 at 8-40; Tr. 14-17; AE E; AE F)

SOR 1.a – Applicant was terminated by his employer on June 6, 2017 for alleged theft of a company laptop. In the June 2017 termination letter, the vice president of government security indicated that Applicant's conduct resulted in a series of security violations as outlined in the company's "Master System Security Plan." The vice president and others saw Applicant in a video on January 25, 2017 removing an unclassified laptop from the storage area. The vice president determined that: (1) Applicant had violated company policy and government security regulations; and (2) Applicant performed a willful action inconsistent with his job duties and classification. The second allegation appears to be a restatement of the first allegation using different words, with the addition of the word "willful." Applicant never saw the final investigation report (June 6, 2017); he saw the termination letter (June 6, 2017) for the first time two weeks before the hearing. He did not dispute the termination because he violated the policy prohibiting his access to the storage areas. However, Applicant was unaware of the change in policy. (GE 3 at 1; GE 4 at 1; Tr. 23-24, 54-57)

Applicant did not steal the laptop. In preparation for a security inspection on January 25, 2017, he was asked to ensure the secure communication equipment in the SCIF was working properly. To check the system, he reviewed the instructions for the secure telephone equipment (STE) which indicated that the phone software should be tested and updated as required. In order to check the software, the phone had to be connected to a laptop and the system checked as necessary. (GE 2 at 2-3; Tr. 24)

Applicant determined that he needed a laptop from the storage area. Based on a specific addendum for a classified customer (which Applicant previously received at an identified date), he had authority to transfer unclassified equipment in and out of SCIF so that he could perform project-related tasks. He disabled some of the functions and turned off the hard drive controller of the laptop. This may have been why, during the subsequent investigation, management thought the hard drive was wiped clean after they experienced a difficult time booting the system and getting the encryption module of the laptop to engage. (Tr. 26-28, 32)

On January 25, 2017, Applicant opened up the storage area (identified as the "storage closet" and "IT Storage area" in the government exhibits) with a key he been provided by the previous facility security officer (FSO) when he was hired in 2013. Applicant carried the laptop and cables from the storage area to the SCIF and started the STE check where he determined that the STE setting was incorrect. After adjusting the setting, the STE phone system began working properly. Applicant provided this explanation of how he used the laptop to solve the STE phone problem to corporate

counsel in March 2017 and to the vice present of government security in April 2017. (GE 2 at 2-3; GE 3 at 2; GE 4 at 1; Tr. 33, 34, 36, 65)

After successfully completing the STE test (January 25, 2017), Applicant learned that the security inspection was still in progress, so he placed the laptop, the cables, and some other equipment in a box outside the SCIF, in a specific area which was not in the unsecured area where other equipment was checked to determine its classification. Because the security inspection was still ongoing, Applicant did not have time to clear the laptop and return it to the storage area as required by standard procedure. Unfortunately, he forgot about the laptop for about a month and a half. (GE 2 at 3; Tr. 30)

On March 9, 2017, corporate counsel and other members of management had a meeting with Applicant about the missing laptop. The counsel presented Applicant with a video dated January 25, 2017, showing him removing a laptop from the storage area. Applicant did not recall taking the laptop. Counsel asked Applicant to ruminate about the laptop's whereabouts, then call the counsel and return it to the director of special programs. Management also interrogated Applicant on how he got the keys for the storage area, but about a week later, dropped that part of the investigation when it was determined Applicant had authority to possess the keys. (GE 2 at 2-3; GE 3 at 2; Tr. 30-35, 59-61)

On approximately March 11, 2017, the security officer at another facility of Applicant's company was having a problem with the STE system, and asked Applicant for assistance. When the security officer mentioned the STE issue, Applicant remembered the location of the missing laptop. He retrieved the laptop from the box outside the SCIF, and made sure it had not been restarted or "booted up." After shutting it down, he called corporate counsel and turned it over to the director of special programs as requested. Applicant learned at a meeting in April 2017 that, unbeknownst to him, there had been a change in corporate policy in 2016 that only government security solutions personnel were allowed access to the storage area. The policy change meant he was no longer permitted access into the storage area. (GE 2 at 2-3; GE 3 at 2; Tr. 28, 30-35, 47, 59-61, 64)

SOR 1.b – In response to Section 13-A Employment Activities, of his August 2017 e-QIP, Applicant stated that his reason for leaving his employment in June 2017 was "terminated employment." In the next block of the section, Applicant answered affirmatively that the employment action occurred in the last 7 years. In the next block requiring a summary of the reasons for leaving the employment, Applicant indicated he was "fired." In response to the reason for being fired, Applicant indicated "failure to follow corporate policy." He indicated in his answer to the SOR that when he submitted the August 2017 e-QIP, the only reason he knew for his June 2017 termination was a violation of corporate policy. In response to the question of why he did not reveal the incident in his e-QIP, Applicant stated that he did not view the event as security-related because he never received a written reprimand. He discovered from his subsequent employer (June 2017 to December 2017) that there was an entry in the DOD's Joint

Personnel Adjudication System (JPAS) for a security incident that he knew nothing about, but was the reason he was required to resubmit an e-QIP. (GE 3; September 2018 answer to SOR; Tr. 43-45, 62-63)

SOR 1.c – As noted earlier in the factual findings, when Applicant provided the March 2018 PSI, he only knew that he was terminated June 2017 for violating company policy. In the March 2018 PSI, he provided details about why he used the laptop and how he retrieved it after remembering where he put the device outside the SCIF. Applicant provided details of the security policies authorizing his access to the SCIF and restoring the STE. When asked about employment issues at his former employer, he provided wide-ranging detail about the laptop investigation between January and June 2017. He also supplied information about the policy change disallowing his access to the storage room. (GE 2 at 2-4; GE 3; September 2018 answer to SOR; Tr. 45-47)

Applicant explained that the vice president of government security wanted to build a large SCIF that would allow different customers (agencies) to use the SCIF area at the same time, but at different classification levels. Applicant told the vice president that customers would not approve the configuration. As Applicant predicted, when the SCIF was completed, other customers declined to use it because they did not approve of the configuration. They also cited a potential lack of control over a specific area within the SCIF. (GE 2 at 2-4; GE 3; September 2018 answer to SOR; Tr. 38-40)

Applicant believes that primary reason he was terminated was that the vice president of government security made him a "scapegoat" after the company spent a large sum of money to build the SCIF, then could not get the secured area certified. (GE 2 at 2-4; GE 3; September 2018 answer to SOR; Tr. 45-47)

Applicant denied that he stole the laptop (SOR 2.a). In late January 2017, during an investigation by management to locate the missing laptop, an audit of the classified systems was conducted and no unusual activity by Applicant was found on the classified systems. Review of building access control logs did not reveal any unusual building activity. Neither SCIF policies nor customer data was compromised. When Applicant recalled where he had left the laptop, he turned it over to the director of special programs. Thus, Applicant placed the laptop in the box, intending to return it to the storage area. He forgot about it, but he did not steal the laptop. (GE 3 at 1-3)

Applicant maintains that he did not misuse technology systems as alleged under SOR 3.a. Rather, he followed all policies and rules and was authorized by the previous security officer to transfer the laptop from the storage area to fix the SCIF system because that was his job. (Tr. 46-47)

Applicant's only other security violation occurred in 2013 with the same employer who terminated him in June 2017. In the 2013 incident, he was assigned to audit classified laptops that were stored in a safe within a restricted area. He removed the laptops from the safe and began auditing them individually according to procedure. Then, he thought he had placed all the laptops back in the safe, but inadvertently left

one laptop unattended in a chair. Later the same day, another employee discovered the unattended laptop and reported it. A two-person audit team determined that no classified information was compromised and the laptop was returned to the safe. Applicant received a written reprimand and was required to review the security policies and procedures to prevent a recurrence. (GE 2 at 4)

Character Evidence

Applicant testified that before he was terminated in June 2017, his performance was very good. He received bonuses and in an unidentified year, he was selected as security person of the year.

Attached to Applicant's September 2018 answer is a character endorsement from the security services team lead indicating that Applicant began working on a project with a federal agency in December 2017. Since that date, Applicant has made significant contributions to the quality of security reviews. His contributions have helped reduce the time necessary to complete the reviews. With his intelligence and experience, the team lead recommends Applicant for a security clearance. (AE A, attachment)

Applicant's friend indicated by letter dated September 27, 2018, that he has known Applicant on a social basis since 2012. In that time, he has learned that Applicant pays a high degree of attention to detail and accuracy. He has impressive computer skills. The friend, who is retired from a federal agency, considers Applicant honest and reliable. (AE D)

Applicant called two witnesses to testify about his character. Both had previously provided letters of support, with one letter is dated in October 2018. Witness B testified that he is retired from a DOD agency. He has held a security clearance since the 1970s. He worked with Applicant for a contractor from 1999 to 2005, when Applicant left to work for another contractor. They have become friends over the years. Witness B considered Applicant as honest, trustworthy, and a good family man. Applicant's computer knowledge has been beneficial for Witness B's children. (AE B; Tr. 74-79)

Witness C currently works for a defense contractor. He has known Applicant for about 33 years since they were in the USN. Even after Applicant told Witness C about the events leading to his job termination in 2017, Witness C still recommends Applicant for a security clearance. (AE C; Tr. 69-73)

Policies

When evaluating an applicant's suitability for a security clearance, the administrative judge must consider the adjudicative guidelines. These guidelines, which are flexible rules of law, apply together with common sense and the general factors of 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 the 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 applicant or proven by Department Counsel. . . ." The applicant has the ultimate burden of persuasion in seeking a favorable security decision.

Analysis

Personal Conduct

The security concern for personal conduct is set forth in AG ¶ 15:

> 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 national security investigative or adjudicative processes. The following will normally result in an unfavorable national security eligibility determination, security clearance action, or cancellation or further processing for national security eligibility.

The potential disqualifying conditions under AG ¶ 16 are:

> (a) deliberate omission, concealment, or falsification of relevant facts from any personnel security questionnaire, personal history statement, or similar form used to conduct investigations, determine employment qualifications, award benefits or status, determine national security eligibility or trustworthiness, or award fiduciary responsibilities;
>
> (b) deliberately providing false or misleading information; or concealing or omitting information, concerning relevant facts to an employer, investigator, security official, competent medical or mental health professional involved in making a recommendation relevant to a national security eligibility determination, or other official government representative;
>
> (c) credible adverse information in several adjudicative areas that is not sufficient for an adverse determination under any other single guideline, but which, when considered as a whole, 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 he may not properly safeguard classified or sensitive information.

On June 6, 2017, Applicant was terminated for alleged theft of a company laptop (SOR 1.a). On January 25, 2017, he was captured on video removing a laptop from a storage area. Throughout the security investigation, Applicant denied stealing the laptop. Throughout the security investigation, he denied violating company policy. Rather, he had a good-faith belief that he was authorized at all times to carry laptops in an out of the SCIF. Applicant was completely forthright with corporate counsel in March 2017 about why he retrieved and used the laptop. (GE 3 at 2) In April 2017, Applicant explained to the vice president of government security that he was authorized to carry laptops in and out of the SCIF. He had not been informed of the policy change restricting access to the storage area to only certain employees. Had he known about the change in corporate policy, he would have complied with those changes. I find Applicant's explanations during the security investigation and at the hearing credible. Because I do not find AG ¶ 16(c) applies, mitigation is not necessary.

SOR 1.b and 1.c will be addressed together since they allege deliberate falsifications by Applicant in his August 2017 e-QIP and March 2018 PSI. I am convinced that the only information that Applicant knew about that caused his June 2017 employment termination was a violation of company policy. That is information he provided on the August 2017 e-QIP. I find his explanation credible. AG ¶ 16(a) does not apply.

Concerning SOR 1.c, Applicant offered a "scapegoat" explanation for why he thought he was terminated. However, this explanation precedes an extensively detailed account of employment issues, including policies, with his former employer between 2013 and June 2017. Given Applicant's credible account of the employment events in his March 2018 PSI, confirmed in his answer to the September 2018 SOR, and at the hearing, I find that he did not deliberately falsify his March 2018 PSI. AG ¶ 16(b) does not apply and a discussion of mitigating conditions is not necessary.

Criminal Conduct

The security concern for criminal conduct is set forth 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.

The potential disqualifying condition under AG ¶ 31 is:

> (b) evidence (including, but not limited to, a credible allegation, an admission, and matters of official record) of criminal conduct, regardless of whether the individual was charged, prosecuted or convicted.

First, AG ¶ 31(b) requires at least evidence of a credible allegation. The Government has not presented a credible allegation that Applicant stole the laptop. *See*

GE 3. The only admission that Applicant has repeatedly made throughout the course of the security investigation and at the hearing has been that he did not steal the laptop. The fact that he was seen on video with the laptop supports Applicant's position that he had authority to enter the SCIF to fix the STE system. He used the laptop, but forgot to return it to the storage area. When he remembered where he put the laptop he immediately contacted corporate counsel and transferred the laptop to the director of programs as requested. Thus, Applicant temporarily placed the laptop at a temporary location with intention of returning the device to the storage area. He forgot about it, but he did not steal it. I find that Applicant's explanation regarding the laptop is credible. AG ¶ 31(b) has not been established and a discussion of the mitigating conditions is not required.

Misuse of Technology Systems

The security concern under AG ¶ 39 is

> 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.

Conditions that may be disqualifying under AG ¶ 40 include:

> (b) unauthorized modification, destruction, or manipulation of, or denial of access to, an information technology system or any data in such a system;
>
> (e) unauthorized use of any information technology system; and
>
> (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.

As corporate information security manager, Applicant violated his employer's policy (change in policy occurred in 2016) restricting access of the storage areas to certain personnel. His unauthorized manipulation of the employer's technology system by retrieving the laptop from the storage closet, making certain adjustments to the laptop, then transporting the laptop to the SCIF to fix the STE system, falls within the scope of AG ¶¶ 40(b), 40(e), and 40(f).

Conditions that may be mitigating under AG ¶ 41 are:

> (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;
>
> (b) the misuse was minor and done solely in the interest of organizational efficiency and effectiveness;
>
> (c) the conduct was unintentional or inadvertent and was followed by a prompt, good-faith effort to correct the situation and by notification to appropriate personnel; and
>
> (d) the misuse was due to improper or inadequate training or unclear instructions.

Applicant's conduct occurred approximately two years ago. The misconduct did not occur under unusual circumstances because Applicant was at work. As the corporate information security manager, Applicant had a good-faith belief that he was authorized to enter and exit the storage area and SCIF with equipment to carry out his job responsibilities. Given Applicant's character evidence, specifically the positive evidence from his current team lead praising his work performance, AG ¶ 41(a) applies.

The circumstances of this case do not fall exactly within AG ¶¶ 41(b), 41(c) and 41(d). However, three mitigating conditions apply in part. While Applicant's employer viewed the entire incident as major, the circumstances show that the violation of corporate policy was minor. *See* the first clause of AG ¶ 41(b). When he remembered where he had placed the laptop, he retrieved it and turned over to management as requested to correct the situation. AG ¶ 41(c) applies in part. Applicant's unauthorized entry into the SCIF to adjust the STE system occurred because he had not been informed of the policy change that occurred less than a year earlier. *See* second clause of AG ¶ 41(d). The government exhibits show that the employer's technology system was not damaged in any manner. Applicant was cooperative throughout his employer's investigation and the government's investigation.

Whole-Person Concept

I have examined the evidence under the personal conduct, criminal conduct, and information technology guidelines with the whole-person concept 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 access to classified information must be an overall common-sense judgment based upon careful consideration of the guidelines and the whole-person concept.

I have weighed the disqualifying and mitigating conditions in light of all the surrounding circumstances of this case. I have evaluated these conditions with the nine factors of the whole person concept. I have considered Applicant's favorable character references that date to his 20-year career in the USN. The one-time policy violation in January 2017 was unfortunate. In Applicant's 40-year history of holding a security clearance, his only security-related incident occurred in 2013, when he left a laptop unattended. He was reprimanded and required to attend a remedial briefing regarding policies to prevent a recurrence. Considering the evidence from an overall commonsense point of view, Applicant has mitigated the security concerns raised by the guidelines for personal conduct, criminal conduct, and misuse of technology systems.

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 E):	FOR APPLICANT
Subparagraphs 1.a-1.c:	For Applicant
Paragraph 2 (Guideline J):	FOR APPLICANT
Subparagraphs 2a:	For Applicant
Paragraph 3 (Guideline M):	FOR APPLICANT
Subparagraph 3.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 security interests of the United States to grant Applicant eligibility for access to classified information. Eligibility for access to classified information is granted.

_____
Paul J. Mason
Administrative Judge