DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 18-01629
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Ross Hyams, Esq., Department Counsel
For Applicant: Leon J. Schacter, Esq.

08/30/2019

_____

Decision

_____

Curry, Marc E., Administrative Judge:

The amount of time that has elapsed since Applicant's security violation, and the circumstances surrounding the violation are insufficient to overcome the security concern, given the nature and seriousness of the transgression. Clearance is denied.

Statement of the Case

On August 24, 2018, the Department of Defense Consolidated Adjudications Facility (DOD CAF) issued a Statement of Reasons (SOR) to Applicant, detailing the security concerns under Guideline K, handling protected information, and Guideline E, personal conduct, explaining why it was unable to find it clearly consistent with the national interest to grant security clearance eligibility. The DOD CAF took the action under Executive Order (EO) 10865, *Safeguarding Classified Information within Industry* (February 20, 1960), as amended; and DOD Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (January 2, 1992), as amended (Directive) and the National Security Adjudicative Guidelines (AG), effective June 8, 2017.

On September 11, 2018, Applicant answered the SOR, admitting subparagraph 1.a, as cross-alleged in subparagraph 2.a, and denying subparagraphs 2.b and 2.c. He

requested a hearing, whereupon on December 10, 2018, the case was assigned to me. On March 18, 2019, DOHA scheduled the hearing for April 10, 2019.

Before the hearing, Department Counsel provided Applicant's counsel with six exhibits (Government Exhibit (GE) 1 through GE 6) that he planned to introduce at the hearing. Applicant's counsel objected to the admissibility of all of the exhibits except GE 1. After considering pre-hearing briefs from both parties, and arguments at the hearing regarding this matter, I admitted GE 1, sustained Applicant's counsel's motion to exclude GE 2, and admitted GE 3 through GE 6, denying his motion to exclude them.

Department Counsel then moved to continue the hearing to allow him the opportunity to procure the testimony of a witness to authenticate GE 2. Counsel for Applicant objected. I granted the motion in part, continuing the case for Department Counsel to procure the authenticating witness, and denied it in part, allowing Applicant's counsel to present the testimony of the two character witnesses who had come to the hearing to testify.

Before continuing the hearing, I also admitted four exhibits, identified as Hearing Exhibits (HE) I through HE IV. HE I and HE II are copies of e-mail correspondence between the parties and me. HE III is the National Industrial Security Program Operating Manual (February 2006, Incorporating Change 2, May 18, 2016). HE IV is Chapter 5, Section 1 of DOD 5220.22-M (February 28, 2006).

On March 18, 2018, DOHA scheduled the completion of the hearing for June 3, 2019. The hearing was held as rescheduled. After considering the testimony of the authenticating witness, I admitted GE 2, over Applicant's counsel's renewed objection. I also received six Applicant exhibits identified as AE A through AE F. At counsel's request, I marked another court exhibit, for identification purpose only, as HE V, DOD Instruction 7050.01, effective October 17, 2017.

At the conclusion of the hearing, I left the record open for ten days to allow parties to supplement their closing arguments. On June 5, 2019, I received a supplementary closing argument from Applicant's counsel, and on June 6, 2019, I received a response from Department Counsel. I appended the e-mailed copies of these submissions as HE I at pages 46 through 50. The transcript (Tr.) of the first part of the hearing was received on April 30, 2019. The transcript of the second part of the hearing was received on June 13, 2019.

Findings of Fact

Applicant is a 52-year-old married man with two teenage children. He earned a Bachelor of Science degree in architecture in 1994, and an associate's degree in project management in 2007. (AE A at 2) He has been working in the information technology field since 1984, and has been a program manager since 2003. He was first granted a security clearance in 2006. (AE A at 2)

Applicant is an engineer who installs and upgrades fiber security systems. (AE C at 1) His current supervisor, who has worked with him in various capacities for 34 years, characterizes him as an exceptional engineer who performs his duties above and beyond the scope of work required by their clients. (AE C at 1)

Applicant worked for his previous employer from 2010 to 2013. (GE 1 at 11) He supervised a team of five engineers and ten technicians as part of a project to upgrade the network systems. (Tr. 75; GE 2) The project was two pronged. It first involved going to several rooms to inventory the network systems and determine which needed to be physically replaced, then replacing the systems that needed to be upgraded. (Tr. 89) Applicant's team worked on the identification and inventory prong of the project. (Tr. 89, 106) Each day, team members went to multiple classified rooms and security closets. Entry to these rooms was controlled by up to two combination locks, depending upon the classification level. (Tr. 90)

Each day, Applicant went to a swipe-access-controlled sensitive compartmented information facility (SCIF) to retrieve the combinations. The combinations that controlled access to SCIFs were in a separate room than the lock combinations for the rooms that housed lower-level classified information. (Tr. 105) Each of the combinations had three numbers.

Because the numbers to the combinations were classified, Applicant could not write them down. Instead, he had to memorize them. After retrieving the combinations and memorizing them, he would pass them along to his team members, who would then go to the respective rooms to execute their assignments. (Tr. 134-135) Combinations could not be disclosed in unclassified facilities.

Memorizing all of these numbers in the proper order was challenging. At most, Applicant had to memorize "30 different numbers in a specific order, couple[d] with nine to eighteen different combinations." (Tr. 106 -107) If he forgot a combination, he had to return to the room where he had originally received it. This could slow the project by 30 minutes. (Tr. 115) In late 2012, an engineer who worked at Applicant's company suggested that he store the combination codes in his personal cell phone. (Tr. 117, 127) He provided Applicant with encryption software to protect the information which Applicant downloaded onto his phone. Applicant did not check with his FSO or supervisor about whether the encryption software had been approved for use by either his employer or the agency. (Tr. 142)

Using the encryption software, Applicant began inputting the classified combinations into his personal cell phone. (Tr. 127) He would later refer to the cell phone for the combinations to help remember them when he provided them to his subordinates. The disclosure of these classified combinations to his subordinates occurred in an unclassified, open office space. (GE 2 at 2) Applicant thought the room was classified because it was secured by a special lock. (Tr. 129) It is unclear from the record how long Applicant obtained and shared classified combinations in this fashion.

In November 2012, the DOD's inspector general's office received an anonymous complaint about Applicant's security practices regarding the classified combinations. (GE 2 at 1; AE F) The anonymous complaint also alleged that Applicant wrote classified combinations in a black book. Applicant denied this allegation about the black book and the investigation includes no finding regarding this allegation. (Tr. 123, 139)

The complaint was referred to the facility and personnel security division of the department where Applicant was performing his contract work. The complaint prompted an investigation that began in April 2013. (GE 6, Enclosure (Enc.) 6; AE F) Subsequently, the then-chief security manager interviewed Applicant. During the interview, he "clearly and freely admitted that he did house those combinations, and he did disclose them to his personnel . . . ." (Tr. 24)

According to the former chief security manager, Applicant and the other contractors received security briefings every month. (Tr. 25) Applicant contended that the security training he received was generic and did not address the subject of storing combinations on personal phones. (Tr. 114) Moreover, he contended storing information on his phone enabled him to get more combinations to his teammates more quickly, without having to return multiple times to the rooms where he was required to go to retrieve them. By promoting efficiency, Applicant "thought it was for the betterment of the team." (Tr. 115)

After completing the investigation in May of 2013, the chief security manager concluded that Applicant's actions caused a compromise of classified combinations. Additionally, he concluded that "contract security officers [were] not properly briefing contractor personnel on their security responsibilities." (GE 2 at 2; AE F) Ultimately he recommended that Applicant's access to classified information be terminated.

Because of Applicant's security violation, the agency had to change all of the combinations. Changing the 400 to 500 combinations required 192 work-hours. (Tr. 27)

The chief security manager who conducted the investigation testified at the hearing. He stated that his investigation into Applicant's improper handling of classified information also included reviewing the guidance involving memorizing multiple combinations. (Tr. 52) As part of the review process, the chief security manager and his team consulted with various work groups that needed access to classified spaces in an effort to ascertain "how [they] could actually assist these people and still keep from having compromises." (Tr. 55) He concluded that the procedure which involved contractors memorizing as many combinations as possible was not a good practice. (Tr. 53) Consequently, the security manager and his staff developed a new policy where "you would have to come to the security office, make your case for a number of combinations and we would be the ones to vet and provide those combinations to you in our classified facilities." (Tr. 55)

On May 22, 2013, Applicant's employer placed him on unpaid administrative leave, pending its investigation. (GE 6, Enc. 3) This decision was reached because Applicant, absent a security clearance, was "not permitted to complete [his] duties as outlined in [his] employment agreement . . ." (GE 6, Enc. 3) As part of the company's out-processing

procedures, he was required to turn in all of his building access keys and badges, and to attend a security debriefing. (GE 6, Enc. 4) In addition, he was instructed that his health benefits were set to terminate within ten days of the unpaid administrative leave notice. (GE 6, Enc. 3) The memo setting forth these instructions does not characterize Applicant's pending departure as a termination.

On March 1, 2016, the FSO of Applicant's former employer responded to a request for background information received from the U.S. Office of Personnel Management, as part of a new clearance investigation. (GE 6; AE F) In his response, the FSO noted that Applicant's continued assertion that he did not receive the proper training to handle the classified information "confirms that he was not, and is not capable of handling classified information because common sense dictates the information he was handling was classified and his handling of it . . . was improper." (AE 6 at 1)

According to an individual whom Applicant supervised on a job prior to the job where the security violation occurred, he was a "serious-minded professional" who made information security "his highest priority." (AE C at 4) He corrected this former subordinate on one occasion, and taught him how "to keep multiple sources of information, floor plans and cut-sheets, securely stored separately, and not together." (AE C at 4) His former supervisor at the job where the security violation occurred characterizes it as an anomaly that does not reflect Applicant's ability to protect classified information. (AE C at 5) He frequently observed Applicant mentoring subordinates on physical security issues. (AE C at 5)

According to one of Applicant's former coworkers who was involved with his termination, Applicant was removed from his position, pending an investigation into the alleged security violation and because there were no other positions available in the company that were commensurate with his experience, credentials, or compensation. (AE D at 1) He considers Applicant to be "honest, very detailed, and passionate about his work." (AE D at 1)

Applicant completed a security clearance application in February 2016. In response to the question whether he had ever been fired, quit after being told he would be fired, left by mutual agreement following charges or allegations of misconduct or unsatisfactory performance, he answered "yes," explaining that he left the position by mutual agreement, as discussed above, for "alleged violation of security procedures that [he] had never received proper training." (GE 1 at 12)

Another question on the February 2016 security application asked whether Applicant had ever received a written warning, been officially reprimanded, suspended, or disciplined for misconduct in the workplace, such as a violation of security policy. He answered, "yes," again referencing the position that he left in 2013, explaining that he was punished for an "alleged violation of security procedures that [he] was never trained on." (GE 1 at 13)

A government investigator interviewed Applicant in March 2017. He told the agent that he left his previous employer by mutual agreement following the security violation

allegations, and that he was eligible for re-hire. (Tr. 152-153) He believed this to be the case because he never was told that he could not return.

Applicant has continued to take security trainings over the years. In March 2019, he completed a counterintelligence training, and later that month, he completed an annual security awareness refresher course. (AE D3 at 1; AE D4 at 1)

Policies

The U.S. Supreme Court has recognized the substantial discretion the Executive Branch has in regulating access to information pertaining to national security, emphasizing that "no one has a 'right' to a security clearance." *Department of the Navy v. Egan*, 484 U.S. 518, 528 (1988). 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 required to be considered in evaluating an applicant's eligibility for access to classified information. These guidelines are not inflexible rules of law. Instead, recognizing the complexities of human behavior, these guidelines are applied together with the factors listed in the adjudicative process. The administrative judge's overall 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 national security eligibility will be resolved in favor of the national security." In reaching this decision, I have drawn only those conclusions that are reasonable, logical, and based on the evidence contained in the record. Under Directive ¶ E3.1.14, the Government must present evidence to establish controverted facts alleged in the SOR. Under Directive ¶ E3.1.15, 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 to obtain a favorable security decision.

A person who seeks access to classified information enters into a fiduciary relationship with the Government predicated upon trust and confidence. This relationship transcends normal duty hours and endures throughout off-duty hours. The Government reposes a high degree of trust and confidence in individuals to whom it grants access to classified information. Decisions include, by necessity, consideration of the possible risk that the applicant may deliberately or inadvertently fail to safeguard classified information. Such decisions entail a certain degree of legally permissible extrapolation about potential, rather than actual, risk of compromise of classified information. Section 7 of Executive Order 10865 provides that decisions shall be "in terms of the national interest and shall in no sense be a determination as to the loyalty of the applicant concerned." *See also* EO

12968, Section 3.1(b) (listing multiple prerequisites for access to classified or sensitive information).

Under the whole-person concept, the administrative judge must consider the totality of an applicant's conduct and all relevant circumstances in light of the nine adjudicative process factors in AG ¶ 2(d), as set forth below:

> (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.

Analysis

Guideline K: Handling Protected Information

The security concerns about handing protected information are set forth in AG ¶ 13:

> Deliberate or 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 security concern

Applicant's storage of classified lock combination codes on his personal cell phone, and his later disclosure of these combinations to subordinates in an unclassified area trigger the application of the following disqualifying conditions under AG ¶ 34:

> (b) collecting or storing protected information in any unauthorized location;
>
> (c) loading, drafting, editing, modifying, storing, transmitting, or otherwise handling protected information, including images, on any unauthorized equipment or medium; and
>
> (g) any failure to comply with rules for the protection of classified or sensitive information.

The chief security officer, who investigated Applicant's security violations, concluded, among other things, that contract security officers were not properly briefing

contractor personnel on their security responsibilities. Moreover, he testified that the procedure which involved contractors memorizing as many combinations as possible was not a good practice, and that Applicant's case was one of the catalysts for reforming the procedure for contractors to obtain access to locked, classified rooms. This raises the issue of whether AG ¶ 35(c), "the security violations were due to improper or inadequate training or unclear instructions," applies.

Regardless of the quality of security clearance training that Applicant received, or the efficacy of the procedure governing the retrieval of classified combination locks, it is axiomatic that storing combinations to locks securing rooms that contain classified information on one's personal cell phone, constitutes an improper handling of classified information. AG ¶ 35(c) does not apply.

In 2019, Applicant took two refresher security courses. AG ¶ 35(b), "the individual responded favorably to counseling or remedial security training and now demonstrates a positive attitude toward the discharge of security responsibilities," applies.

Applicant's security violation occurred six years ago. However it was egregious, as it compromised the combinations to more than 400 locks, all of which had to be replaced at a cost of 192 work hours. Given the nature and scope of his transgression, I am unable to conclude that AG ¶ 35(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," applies. Applicant has failed to mitigate the security concern related to handling protected information.

Guideline E, Personal Conduct

Under this guideline, "conduct involving questionable judgment, lack of candor, dishonesty, or unwillingness to comply with rules and regulations can raise questions about an individual's reliability, trustworthiness, and ability to protect classified or sensitive information." (AG ¶ 15) Applicant's conduct is disqualifying under this guideline for the same reasons as they are disqualifying under the guideline governing the handling of protected information, as explained above. Applicant's alleged falsifications, as alleged in subparagraphs 2.b and 2.c, raise the issue of whether the following disqualifying conditions under AG ¶ 16 apply:

> (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, and
>
> (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.

Applicant answered "yes," in response to the questions on the security clearance application asking him whether he had either left a position under adverse circumstances, or whether he had ever been disciplined, reprimanded, or suspended from a job. He also identified the employer involved and the date of his departure. His assertion that the security violations occurred because of a lack of proper training was an expression of his subjective belief, not a falsification. I conclude Applicant did not falsify his 2016 security clearance application.

Given the testimony of one of the individuals involved with Applicant's termination from his employment, vouching for his honesty, I am also persuaded that he was not attempting to mislead the investigator in March 2017 when he stated he left the job by mutual agreement. I conclude there are no personal conduct issues related to falsification.

Applicant's mishandling of protected information is disqualifying, as cross-alleged in Paragraph 2, for the same reasons it is disqualifying under the guideline governing the handling of protected information, as discussed earlier in the decision.

Whole-Person Concept

Applicant has many positive attributes. Historically, he has been a good performer on the job. Many individuals, including an individual from his former company where Applicant left after his clearance was suspended who was involved in his termination, vouched for his character. Moreover, contrary to the SOR allegations, he did not intend to mislead anyone in the investigative process when he completed his security clearance application and later, when he interviewed with an agent. Conversely, mishandling of classified information strikes at the heart of the security process, and as such, requires applicants to overcome a very heavy burden to mitigate. When viewed in this context, Applicant's security violation is simply too egregious for me to conclude without any doubt that such a violation would not recur in the future. I conclude that Applicant has failed to carry the burden.

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 E:	AGAINST APPLICANT
Subparagraph 2.a:	Against Applicant

Subparagraph 2.b – 2.c: For Applicant

Conclusion

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

_____
Marc E. Curry
Administrative Judge