



**DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS**



In the matter of:)	
)	
)	ISCR Case No. 17-03798
)	
Applicant for Security Clearance)	

Appearances

For Government: Nichole A. Smith, Esq., Department Counsel
For Applicant: *Pro se*

02/08/2019

Decision

CREAN, Thomas M., Administrative Judge:

Applicant provided sufficient information to mitigate security concerns for handling protected information under Guideline K. Eligibility for access to classified information is granted.

Statement of the Case

Applicant was granted eligibility for access to classified information in June 1984. Applicant submitted his latest Electronic Questionnaires for Investigations Processing (e-QIP) to retain his eligibility for access to classified information required for employment by a defense contractor on July 12, 2017. (Government Exhibit (GX 1))

An incident report in the Joint Personnel Adjudication system (JPAS), dated April 17, 2017, listed three security violations by Applicant. (GX 2) The first incident was on November 29, 2016; the second was on January 9, 2017; and the third was on March 8, 2017. On November 27, 2017, the Department of Defense issued to Applicant a Statement of Reason (SOR) detailing security concerns for protecting protected information under Guideline K. The action was taken under Executive Order (E.O.)

10865, *Safeguarding Classified Information within Industry* (February 20, 1960), as amended; Department of Defense Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (January 2, 1992), as amended (Directive); and the adjudicative guidelines (AG) effective in the DOD on June 8, 2017.

Applicant answered the SOR on December 15, 2017, admitting the three allegations of deliberate or negligent failure to comply with rules and regulations for handling protected information under Guideline K. He provided explanations for his mishandling of protected information on the three occasions. Department Counsel was prepared to proceed on January 29, 2018, and I was assigned the case on July 14, 2018. The Defense Office of Hearings and Appeals (DOHA) issued a Notice of Hearing on September 20, 2018, for a hearing on November 14, 2018. I convened the hearing as scheduled. The Government's two exhibits (GX 1 and 2) were admitted without objection. Applicant and three witnesses testified. DOHA received the transcript (Tr.) of the hearing on November 26, 2018.

Findings of Fact

Applicant's admissions are included in my findings of fact. After a thorough review of the pleadings, hearing transcript, and exhibits, I make the following additional findings of fact. Applicant is 60 years old. He received a Bachelor's Degree in Computer Science in February 1981. He has never served in the military. He has worked as an Oracle data base administrator for defense contractors since 2007. He first married in 1981, divorced in 1993, and married again in 2002. He has five children. (GX 1, e-QIP, dated July 12, 2017)

Some of Applicant's work was performed in a Special Compartmented Information Facility (SCIF). The SOR alleges three incidents of Applicant failing to properly secure the door to the SCIF as required by security procedures. There was no compromise of classified information as a result of the incidents.

Applicant had shoulder surgery on October 4, 2016. He was in pain for a few weeks after the surgery, not sleeping well, and taking narcotic pain relievers. He was cleared by his doctor to return to work by late October, 2016. He continued with physical therapy until early spring 2017. (Tr. 11-14)

The first incident (SOR 1.a) was on November 29, 2016. Applicant admitted he did not properly secure the door to the SCIF. The required procedure was for the last person to use the SCIF in a day to lock the door by spinning the dial, setting the alarm, and signing the security check sheet. If you were not the last person to use the SCIF in a day, an individual just closed the door and spun the combinations locking dial. There was no requirement to set the alarm or sign a security check sheet.

On November 29, 2016, Applicant did not believe he was the last person that would use the SCIF that day. However, he did not check with the person that he believed would use the SCIF after him to be assured that some would follow him to use

the SCIF. Applicant just closed the door and spun the dial. He did not set the alarm or sign the check sheet. The failure to set the alarm and sign the check sheet was discovered later that evening by building security. Applicant was verbally counseled by his supervisor and reread the security procedure guide. (Tr. 14-18)

The second incident occurred on January 9, 2017. Applicant's wife called him at about 1730, and told him that there was an emergency issue with one of his children. He left work immediately to assist his wife. The SCIF was not secured and the proper procedures were not followed. Applicant admitted he was the last person in the office and should have ensured that the SCIF was secured. He stated he had no excuse and he should have locked the SCIF. He received a written warning from his supervisor and was required to receive extra training on open and close procedures. He also received an additional security briefing. (Tr. 18-20)

The third incident happened on March 8, 2017. Applicant could not explain why he did not secure the facility before he departed. He was still in some pain and was receiving physical therapy. But he still had no idea why he did not properly secure the facility that night. (Tr. 20-21)

Applicant no longer works on a contract that requires him to open and close a SCIF. However, he has thought of procedures he can institute himself to assist him in remembering to follow the proper procedures to open and close a facility in the future. (Tr. 21-23)

Applicant's supervisor at the time of the three incidents testified that he was aware that Applicant had surgery in October 2016, was in pain for a time, and taking medication. Applicant was not the only employee that had an issue with securing the SCIF. He was informed by building security when the SCIF was not properly locked. He discussed the first incident with Applicant and determined that he did not need additional training. He decided that their discussion would be sufficient counseling. He had no concern at that time that there would be a similar incident. Applicant did not tell him that his pain was a factor in his failure to secure the facility.

On the second incident, He gave Applicant a written reprimand. He did not remember any reason Applicant provided for his failure the follow procedures. On the third incident, Applicant could not provide a reason for his failure to secure the room. Applicant was upset that he did not lock the room. As a result of this incident, the witness removed Applicant's access to the room. There have been no other security incidents involving Applicant either before or after these events. (Tr. 30-38)

One of Applicant's coworkers testified that he has worked with Applicant since 2015. He knows that Applicant had surgery in October 2016. At the time, Applicant looked like he was in pain and had limited sleep. The witness was only told that there were lapses in properly securing the SCIF. He also knew that Applicant was upset when he realized that he had not properly security the SCIF. At present, Applicant is working

on a non-secure program and does not require access to classified information. He is not aware of any other security breach incidents involving Applicant. (Tr. 39-43)

Applicant's current supervisor testified that he has worked with Applicant for about 18 months. The project they are working does not require them to have open and closing privileges. Applicant is security aware and careful with his work product. His skill set is very good. (Tr. 43-47)

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 must 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 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(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 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 for obtaining 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 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 and sensitive information)

Analysis

Handling Protected Information:

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 three times failed to follow the proper method of securing a SCIF. He was counseled after the first incident and received a written reprimand after the second incident. His failures to properly follow the administrative procedures for securing the SCIF, in spite of counseling, raises the following protected information disqualifying conditions under AG ¶ 34:

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

(h) negligence or lax security practices that persist despite counseling by management.

There is no evidence in the case file to establish that Applicant's failure to properly secure the SCIF resulted in any damage to the national security. In fact, the evidence shows that there was no compromise of classified information. The disqualifying condition at AG ¶34 (i) (failure to comply with rules and regulations that result in damage to the national security, regardless of whether it was deliberate or negligence) is not raised.

I have considered the following mitigating conditions under (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;

(b) the individual responded favorably to counseling or remedial security training and now demonstrates a positive attitude towards the discharge of security responsibilities;

(c) the security violations were due to improper or inadequate training or unclear instructions; and

(d) the violation was inadvertent, it was properly reported, there is no evidence of compromise, and it does not suggest a pattern.

The mitigating conditions apply. Applicant violations were acts of omission not commission. He violated administrative rules in the proper method to lock and secure a SCIF. Applicant had open and close privileges for a SCIF for many years with no other reported violations. The three incidents happened in a four month period, the last about two years ago. There has not been a violation of security procedures by Applicant since. The three violations are not recent and frequent. There have been only these three security procedure violations by Applicant in over 30 years of holding a security clearance. The three violations were while Applicant was in pain from a shoulder surgery and while taking narcotic and other pain medications. The violations are not likely to happen again. Based on the testimony of his supervisor, Applicant responded favorably to counseling. He was warned and counseled. He showed remorse for his violations and responded favorably to the counseling. Applicant presented sufficient information to mitigate the allegations of mishandling protected information by negligently not following proper procedure for securing a SCIF.

Whole-Person Concept

Under the whole-person concept, an administrative judge must evaluate an applicant's eligibility for access to classified information 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 access to classified information must be an overall common-sense 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 considered Applicant's many years of working for defense contractors. Applicant's failure to follow the proper administrative procedures for securing a SCIF was not a deliberate act but an act of omission. Under the circumstances, his conduct does not raise questions about his judgment, reliability, trustworthiness, and ability to comply with rules and regulations. He adequately articulated the circumstances and reasons for his mishandling of the proper procedures and mitigated the security violations. Overall, the record evidence leaves me without questions and doubts concerning Applicant's judgment, reliability, and trustworthiness. He established his suitability for access to classified information. For all these reasons, I conclude Applicant mitigated the security concerns arising from mishandling of protected information.

Formal Findings

Formal findings for or against Applicant on the allegations set forth in the SOR, as required by section E3.1.25 of Enclosure 3 of the Directive, are:

Paragraph 1, Guideline K: FOR APPLICANT

Subparagraphs 1.a -1.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 access to classified information. Eligibility for access to classified information is granted.

THOMAS M. CREAN
Administrative Judge