



DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS



In the matter of:)
)
) ISCR Case No. 20-00659
)
Applicant for Security Clearance)

Appearances

For Government: Daniel O’Reilly, Esq., Department Counsel
For Applicant: Kristen E. Ittig, Esq.

11/01/2021

Decision

RIVERA, Juan J., Administrative Judge:

Applicant mitigated the security concerns raised by his handling of protected information. Clearance is granted.

Statement of the Case

Applicant submitted his most recent security clearance application (SCA) on May 24, 2018 (Government exhibit (GE) 1). He was interviewed by government investigators in March 2019, and answered a set of interrogatories from the Defense Office of Hearings and Appeals (DOHA) in April 2020. (GE 2).

After reviewing the information gathered during the background investigation, the Defense Counterintelligence and Security Agency Consolidated Adjudications Facility (DOD CAF) issued Applicant a Statement of Reasons (SOR) on October 30, 2020, alleging security concerns under Guideline K (handling protected information). Applicant answered the SOR on November 20, 2020, and requested a hearing before a DOHA administrative judge.

DOHA assigned the case to me on February 25, 2021, and issued a notice of hearing on July 13, 2021, setting a video teleconference hearing for July 27, 2021. At the hearing, the Government offered 10 exhibits (GE 1 through 10). All exhibits were admitted into the record without any objections, except for GE 10 (Government's discovery letter mailed to Applicant on March 3, 2021), which was marked and made part of the record, but it is not substantive evidence.

Applicant testified as reflected in a transcript (Tr.) received by DOHA on August 9, 2021. Before the hearing, Applicant submitted via email five documents marked as Applicant's exhibits (AE) 1 through 5. Applicant's exhibits were admitted and made part of the record without objections.

Findings of Fact

The SOR alleged under Guideline K that Applicant committed seven security infractions between April 2017 and October 2019, and a security violation for accumulating more than four security infractions in a 12-month period in March 2018. Applicant admitted the six security infractions for entering a prohibited area with his cell phone (SOR ¶¶ 1.a – c, and f – h). He denied that he improperly marked classified documents in March 2018 (SOR ¶ 1.d), and that he failed to store classified documents in an approved container in March 2018 (SOR ¶ 1.e).

Applicant's SOR admissions and those at his hearing are incorporated into my findings of fact. After a thorough review of all the record evidence, I make the following additional findings of fact:

Applicant, 64, graduated from high school, attended college, and received his bachelor's degree in 1980. Since then, he has completed technical certifications related to his area of expertise in supply chain management. He has worked for different federal contractors since 1979. He has been working for his current employer and clearance sponsor, a federal contractor, since 2007. He married in 2002, and has three adult daughters and two grandchildren. (Tr. 15)

After Applicant was granted eligibility for a clearance for the first time in 2015, he received security training and learned that he was prohibited from bringing a cell phone into a classified area. Since then, he has participated in annual security refresher training, reinforcing the security rules. His most recent security refresher training occurred in May 2021. (AE 2; GE 6)

Applicant testified that all of his cell phone security infractions were accidental. The phone security infractions were caused by his desire to be diligent when responding to requests for support, meetings, or a last-minute tasking in the classified area. He explained that he has two offices, one within the "green area" (unclassified) and the other inside the "red area" where all classified information is handled. He would walk into the red area with his cell phone in his pocket. After a couple of minutes, he

realized his security infraction and he would immediately report the incident and surrender his phone to his facility security officer (FSO). After each occasion, his phone was inspected by security officials to ensure that no classified information was compromised. (GE 3)

After the first three infractions in April, July, and October 2017, Applicant modified his behavior and started to leave his cell phone in his car. He did not have any more phone infractions until July and October 2019. Shortly before his July 2019 infraction, he started to bring his cell phone to work because he needed to coordinate with and help his wife with her medical appointments and care of a grandchild. After his last phone infraction in October 2019, Applicant again modified his behavior and started to connect his phone to its charger and to leave it in the green office on top of his desk. He has not incurred any additional phone infractions after October 2019.

Applicant denied SOR ¶ 1.d, alleging that he improperly marked classified documents and received a security infraction in March 2018. (Two identical pages were marked differently, and a third page was unmarked.) He also denied SOR ¶ 1.e, alleging that he failed to properly secure a classified document in March 2018. (Classified documents were found in multiple places in his cubicle.) (GE 3)

Applicant explained that he shared a cubicle with another employee. The cubicle had two computer desks with their respective overhead bins. The computers and the area were also used by other company employees passing through. Applicant claimed one of the computers and overhead bin as his area, kept it clean, and maintained it organized. He did not manage or clean the other cubicle used by a fellow employee.

In March 2018, a company internal audit discovered unattended classified documents and mismarked classified documents in the bin adjacent to Applicant's claimed area. According to the company records, the computer and bin area where the unattended and mismarked classified documents were found had been assigned to him. Applicant testified that neither he nor his co-worker knew they had been assigned a particular computer and bin area. After taking responsibility for the security infractions, Applicant assumed control of his assigned area and cleaned and organized it. He denied mismarking the document or improperly storing the classified document in the bin. (Tr. 31-35)

An incident report states that "there was no known compromise of classified information because the incident was within a secure facility, but open storage is not allowed". (GE 9) Applicant accumulated more than four security infractions within a 12-month period, and according to company policy, such behavior established a reportable security violation. (SOR ¶ 1.f)

Applicant has done well with his company. He testified that he has always received top ratings in his performance evaluations. (Tr. 20-21) His supervisor considers him to be a valued team member, a trusted employee, and the go-to person

for several company projects. (AE 1) He has established a strong reputation and is respected by peers and employers for his dedication, trustworthiness, and professionalism. His supervisor intends to keep Applicant within her organization even if he were to lose his clearance eligibility. (AE 3)

Applicant's company information systems security officer (ISSO) submitted a strong letter endorsing his eligibility for a clearance. (AE 4) He has interacted with Applicant for the last two years. In his opinion, Applicant has demonstrated honesty, trustworthiness, and his ability to follow rules. He believes that Applicant displays a positive attitude and a strong work ethic. He believes that Applicant voluntarily disclosed all of his accidental infractions because he is honest and follows the rules. He highlighted that Applicant was counseled and he changed his habits. As of the date of his letter in June 2021, Applicant had not had any recent infractions.

Applicant's facility security officer (FSO) and industrial security manager also submitted a letter endorsing his eligibility for a clearance. (AE 5) The FSO previously held the position of ISSO, and was aware of Applicant's security infractions. The FSO noted that Applicant always self-reported his security infractions and notified the security team of his mistakes. He believes Applicant understands the rules and is willing to hold himself accountable. The FSO believes Applicant is one of the most honest people he has ever encountered. He recommends Applicant for a clearance without hesitation.

Applicant expressed sincere remorse for his security infractions and violation. He believes that he voluntarily reported his infractions because of the training he has received since 2015, and the annual security training refresher courses. (Ge 6) He believes that he now has a system in place that has been working since October 2019, to make sure that he does not have any future infractions. He promised to do his best to avoid any future infractions. He is concerned with the security of the United States and would never do anything to jeopardize national security.

Policies

The SOR was issued under Executive Order 10865, *Safeguarding Classified Information Within Industry* (February 20, 1960), as amended; DOD Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (Directive) (January 2, 1992), as amended; and the *National Security Adjudicative Guidelines for Determining Eligibility for Access to Classified Information or Eligibility to Hold a Sensitive Position* (AGs), applicable to all adjudicative decisions issued on or after June 8, 2017.

Eligibility for access to classified information may be granted "only upon a finding that it is clearly consistent with the national interest to do so." Exec. Or. 10865, *Safeguarding Classified Information within Industry* § 2 (Feb. 20, 1960), as amended. The U.S. Supreme Court has recognized the substantial discretion of the Executive

Branch 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).

The AG list disqualifying and mitigating conditions for evaluating a person’s suitability for access to classified information. Any one disqualifying or mitigating condition is not, by itself, conclusive. However, the AG should be followed where a case can be measured against them, as they represent policy guidance governing access to classified information. Each decision must reflect a fair, impartial, and commonsense consideration of the whole person and the factors listed in SEAD 4, App. A ¶¶ 2(d) and 2(f). All available, reliable information about the person, past and present, favorable and unfavorable, must be considered.

Security clearance decisions resolve whether it is clearly consistent with the national interest to grant or continue an applicant’s security clearance. The Government must prove, by substantial evidence, controverted facts alleged in the SOR. If it does, the burden shifts to the applicant to rebut, explain, extenuate, or mitigate the facts. The applicant bears the heavy burden of demonstrating that it is clearly consistent with the national interest to grant or continue his or her security clearance.

Persons with access to classified information enter into a fiduciary relationship with the Government based on trust and confidence. Thus, the Government has a compelling interest in ensuring each applicant possesses the requisite judgment, reliability, and trustworthiness of those who must protect national interest as their own. The “clearly consistent with the national interest” standard compels resolution of any reasonable doubt about an applicant’s suitability for access in favor of the Government. “[S]ecurity clearance determinations should err, if they must, on the side of denials.” *Egan*, 484 U.S. at 531; SEAD 4, ¶ E(4); SEAD 4, App. A, ¶¶ 1(d) and 2(b). Clearance decisions are not a determination of the loyalty of the applicant concerned. They are merely an indication that the applicant has or has not met the strict guidelines the Government has established for issuing a clearance.

Analysis

Guideline K: Handling Protected Information

Under AG ¶ 33 the security concern is that:

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.

Security clearance cases require administrative judges to assess whether an applicant has the requisite good judgment, reliability, and trustworthiness to be entrusted with classified information.

Applicant inadvertently entered a secured (prohibited) area with his phone in April, July, and October 2017, and received three security infractions (SOR ¶¶ 1.a – c). He received a security infraction for improperly marking classified documents (SOR ¶ 1.d), and another for failure to store classified documents in an approved container in March 2018 (SOR ¶ 1.e). He received a security violation for accumulating more than four security infractions in a 12-month period in March 2018 (SOR ¶ 1.f). He inadvertently entered a secured area with his phone in July and October 2019, and received two security infractions (SOR ¶¶ 1.g and h).

Applicant's violations of security rules and procedures raise the following Guideline K security concern under AG ¶ 34:

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

The conditions that could mitigate the security concerns under AG ¶ 35 include:

(a): so much time has elapsed since the behavior, or it happened so infrequently or under such unusual circumstances that it is unlikely to recur or 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 toward the discharge of security responsibilities; and

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

Applicant voluntarily disclosed all of his phone security infractions immediately to his FSO and surrendered his phone for inspection. A review of the phone revealed no classified or sensitive information on the phone. The security personnel considered the compromise of classified information "possible, but not probable." After each incident, Applicant was retrained about the prohibition of bringing cell phones into secured areas. Additionally, he has participated in annual refresher security training since 2015.

After the first three security infractions, Applicant developed practical measures to prevent him from bringing the phone into the secured area (leaving the phone in his car). His method worked until he started bringing the phone with him to the office to communicate with his wife. After the two 2019 phone security infractions, Applicant modified his behavior and started to leave his cell phone in his office plugged to its

charging station. The new system has worked for him. He has not had any additional phone security infractions after October 2019. Considering Applicant's testimony, his security retraining, his positive attitude toward following rules and procedures, and the statements of his supervisor and two company security officials, I believe that the security infraction violations occurred under circumstances unlikely to recur.

Concerning his security infractions for improperly marking classified documents and for his failure to store classified documents in an approved container, there is no evidence of any similar security violations after 2018. Although Applicant claimed someone else left the documents in his office area, he took responsibility for the infractions, cleaned the office area, and organized it to prevent any additional infractions. He acknowledged his mistakes and has learned from them. I find the infractions occurred under circumstances unlikely to recur, and he participated in remedial training and certifications. Applicant is now more aware and cognizant of his responsibility to protect classified information.

Considering the evidence as a whole, I find Applicant's violations happened under such circumstances that are unlikely to recur and are mitigated by the passage of time. His reference statements and his performance evaluation report show that he established a strong reputation for following and complying with security rules and regulations. He established a positive attitude toward the discharge of his security responsibilities. There is documentary evidence of yearly security training up until 2021 to prevent such security infractions in the future. I find that his past security infractions do not cast doubt on his current reliability, trustworthiness, or good judgment. AG ¶¶ 35(a), (b), and (d) apply. The evidence is sufficient to mitigate the security concerns raised by his handling of protected information.

Whole-Person Concept

I considered the potentially disqualifying and mitigating conditions in light of all the facts and circumstances surrounding this case, and under the whole-person concept. AG ¶¶ 2(a) and 2(d). I have incorporated my comments under Guideline K in my whole-person analysis. Some of these factors were addressed under those guidelines, but some warrant additional comment.

Applicant, 64, has been working for federal contractors since 1997, and for his current employer and clearance sponsor since 2007. He was granted clearance eligibility in 2015.

Applicant's references attested to his professionalism, skills, knowledge, leadership, and noted that he is considered an exceptional employee. Both the ISSO and the FSO noted that Applicant always self-reported his security infractions and notified the security team of his mistakes. They believe Applicant understand the rules and is willing to hold himself accountable. They both consider Applicant as one of the most honest people they have ever encountered. Both recommended Applicant for a

clearance without hesitation. Handling protected information security concerns are mitigated. Clearance is granted.

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.h:	For Applicant

Conclusion

In light of all 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's eligibility for a security clearance. Clearance is granted.

JUAN J. RIVERA
Administrative Judge