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

| | | |
|---|---|---|
| In the matter of: | ) | |
| | ) | |
| | ) | ISCR Case No. 15-01205 |
| | ) | |
| | ) | |
| Applicant for Security Clearance | ) | |

## Appearances

For Government: Andrew Henderson, Esq., Department Counsel
For Applicant: Arran Treadway, Esq.

November 23, 2016

_____

## Decision

_____

GOLDSTEIN, Jennifer I., Administrative Judge:

Applicant committed 19 security infractions between 1997 and 2012. However, since September 2012, he has been properly medicated for Attention Deficit Disorder (ADD) and has not had another violation. He demonstrated a positive attitude toward his security obligations. Future infractions are unlikely. Security concerns under Guideline M and K were mitigated. Eligibility for access to classified information is granted.

## Statement of the Case

On March 28, 2016, in accordance with DoD Directive 5220.6, as amended (Directive), the Department of Defense issued Applicant a Statement of Reasons (SOR) alleging facts that raise security concerns under the Guidelines for Use of Information Technology Systems, and Handling Protected Information. The SOR further informed Applicant that based on information available to the government, DoD adjudicators could not make the preliminary affirmative finding that it is clearly consistent with the national interest to grant or continue Applicant's security clearance.

Applicant answered the SOR on April 13, 2016, and requested a hearing before an administrative judge. The case was assigned to me on June 13, 2016. The Defense Office of Hearings and Appeals (DOHA) issued a notice of hearing on June 16, 2016, scheduling the hearing for August 10, 2016. The hearing was convened as scheduled. The Government offered Exhibits (GE) 1 through 3, which were admitted without objection. Applicant offered Exhibits (AE) A through D, which were admitted without objection. Applicant testified on his own behalf and called one witness. DOHA received the transcript of the hearings (Tr.) on August 19, 2016.

## Findings of Fact

Applicant admitted all of the SOR allegations. (Answer.) After a thorough and careful review of the pleadings, exhibits, and testimony, I make the following findings of fact.

Applicant is a 60-year-old employee of a defense contractor. He is divorced and has two adult children. He has a bachelor's degree. He has worked for his employer, or its predecessor, since 1982. He has held a security clearance since approximately 1983. (GE 1; Tr. 22, 23, 37, 42-43.)

Applicant is alleged to have committed 18[1] separate security infractions[2] between February 2008 and July 2012. The infractions can be categorized into three groups. He failed to logoff his classified computer, located inside a Sensitive Compartmented Information Facility (SCIF) on 14 occasions between February 2008 and April 2011. He brought his cell phone into the SCIF on three occasions between October 2011 and July 2012. He also left classified material on his desk and unsecured inside the SCIF once, in August 2009. He received verbal warnings for each of these infractions. (GE 2; GE 3; Tr. 39.)

Applicant attributes his multiple security infractions to his changing routine during that time period. He was required to frequently travel between an unclassified contractor's facility and the SCIF. If he was at the contractor's facility at the end of the day, he sometimes forgot to go back to the SCIF and logoff of his computer.[3] He was not used to working in a SCIF, as all previous classified work had been done in a different setting. He also forgot to take his cell phone out of his pocket when he entered the SCIF on three occasions. He self-reported these infractions. The classified material that he mistakenly left on his desk was in a grey folder, which matched the color of the desk and he overlooked it when cleaning up that day. He candidly accepted responsibly for all of these errors. He was provided verbal counseling from a senior member of the facility security office as a result of all of these incidents. (Tr. 19, 25, 33-35, 41, 44-46.)

[1] Applicant had a total of 19 infractions during his career including an August 2007 cell phone infraction, but this infraction was not alleged on the SOR. (GE 2.)

[2] Applicant's Facility Security Officer (FSO) testified that the infractions did not rise to the level of violations because the probability "of compromise was low at best, to zero." (Tr. 60.)

[3] The computer automatically locked when unattended. (Tr. 19-21.)

Applicant documented that he suffers from ADD. Between February 2008 and July 2012, he was on medication to help with this disorder, but the medication was not working properly. Applicant was having difficulties with attention, concentration, and organization. In September 2012 his Psychiatrist prescribed Applicant a new medication, as documented in a letter from his treating Psychiatrist, which proved to be much more effective in managing his ADD. Since starting the new medication Applicant's "concentration significantly improved." (AE A.) Applicant takes his medication daily and is compliant with his treatment. (Tr. 21, 27-28, 46-49.)

Applicant has not had any additional infractions since July 2012. He takes his security obligations seriously and utilizes several tools to help avoid future infractions, including an activity security checklist, a flashing reminder on his computer screen, and numerous physical pat downs of himself to avoid cell phone infractions. Additionally, his company now utilizes an auto-logoff feature that prohibits future log-off infections, which it instituted as an industry "best practices" feature. (AE C; AE D; Tr. 29-32, 36, 49-52.) He stated:

> It's my job to protect classified information. It's my job to follow the rules. It's my job to make sure that [employer] is not put in a bad light with our customer by my poor performance. So, it was also clear to me that the infractions which were part of the angst during that time, at some point, this can't be acceptable. I mean I don't need somebody to tell me that there's a limit to say that this isn't a good thing. You know, I recognized that at the time. So, it was my personal motivation that really drove me. [Employer] expects me to adhere to policy, and they expressed that to me each and every time. And they worked with me to do that. And eventually, it worked. (Tr. 40-41.)

Applicant's FSO testified on Applicant's behalf. He indicated that "for a little over four years . . . [Applicant] has been following security protocol to a tee," and he "endorses" Applicant for a security clearance. (Tr. 60, 70.) Applicant's performance evaluations reflect that Applicant either meets and/or exceeds all expectations set out in his objectives. (AE B; Tr. 25.)

## 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 the adjudicative process. The administrative judge's overarching 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 access to classified information 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 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 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 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 M, Use of Information Technology Systems

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

> Noncompliance with rules, procedure, 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 Systems include all related computer hardware, software, firmware, and data used for the communication, transmission, processing, manipulation, storage, or protection of information.

AG ¶ 40 describes conditions that could raise a security concern and may be disqualifying. The following disqualifying condition is potentially applicable:

> (g) negligence or lax security habits in handling information technology that persist despite counseling by management.

Applicant committed 14 infractions by failing to logoff his computer, and 3 infractions for bringing his cell phone into the SCIF, over the course of five years. After each infraction, he received verbal counseling. The above disqualifying condition has been established.

AG ¶ 41 provides conditions that could mitigate security concerns. The following are potentially applicable:

> (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; and
>
> (c) the conduct was unintentional or inadvertent and was followed by a prompt, good-faith effort to correct the situation and by notification of supervisor.

Applicant acknowledged his inadvertent errors and takes his security obligations seriously. He self-reported all of the cell phone incidents. He has taken corrective actions, including a checklist and a pat-down routine that are aimed at prohibiting future infractions. He has found an effective medicine to treat his ADD. He has now gone four years without any further infractions. He established that similar circumstances are unlikely to recur. Further, his conduct over the past four years demonstrates that he is currently reliable, trustworthy, and uses good judgment. The misuse was a serious event, which occurred over a five-year time frame, but Applicant has corrected his behavior. Both of the above mitigating conditions apply.

**Guideline K, Handling Protected Information**

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

> Deliberate or negligent failure to comply with rules and regulations for protecting classified or other sensitive information raises doubt about an individual's trustworthiness, judgment, reliability, or willingness and ability to safeguard such information, and is a serious security concern.

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

> (b) collecting or storing classified or other protected information at home or in any other unauthorized location;
>
> (g) any failure to comply with rules for the protection of classified or other sensitive information; and
>
> (h) negligence or lax security habits that persist despite counseling by management.

Applicant received a verbal warning in 2009 for his failure to properly secure classified material. The above disqualifying conditions have been established.

AG ¶ 35 provides conditions that could mitigate security concerns. The following are potentially applicable:

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

Applicant had been trained on the security requirements, but was negligent in carrying out his duties with respect to leaving the classified document unsecured, the cell phone infractions, and the logoff infractions.[4] However, he has demonstrated a positive attitude toward his security responsibilities, and has been extremely honest in reporting his infractions. His attention to detail that would ensure no future spills of classified or sensitive information occur has improved since switching medication for ADD in September 2012. No further infraction has occurred since that change in medication. He has responded favorably to the counseling for his infractions. Applicant's actions are unlikely to recur, despite the high number of infractions from 2007 to 2012. Applicant has the requisite good judgment needed to properly safeguard classified and sensitive information.

**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(a):

[4] The cell phone infractions and the logoff infractions were not alleged as disqualifying conduct under Guideline K, but are appropriate to be considered in a discussion of mitigation.

> (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 pertinent facts and circumstances surrounding this case. I have incorporated my comments under Guidelines M and K in my whole-person analysis. Some of the factors in AG ¶ 2(a) were addressed under those guidelines, but some warrant additional comment. Applicant has a long history of working in the defense industry, and is respected by his FSO, who testified on his behalf. He performs well at his job. He has not had any violations since 2012, and future infractions are unlikely. Overall, the record evidence leaves me without serious questions or doubts as to Applicant's eligibility and suitability for a security clearance. For all these reasons, I conclude Applicant mitigated the Use of Information Technology Systems, and Handling Protected Information security concerns.

## 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 M: | FOR APPLICANT |
| Subparagraph 1.a through 1.q: | For Applicant |
| Paragraph 2, Guideline K: | FOR APPLICANT |
| Subparagraph 2.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 interest to grant Applicant eligibility for a security clearance. Eligibility for access to classified information is granted.

_____
Jennifer I. Goldstein
Administrative Judge