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

| | | |
|---|---|---|
| In the matter of: | ) | |
| | ) | |
| | ) | ISCR Case No. 15-08162 |
| | ) | |
| Applicant for Security Clearance | ) | |

## Appearances

For Government: Bryan J. Olmos, Esq., Department Counsel
For Applicant: Ryan C. Nerney, Esq.

08/14/2017

## Decision

LOUGHRAN, Edward W., Administrative Judge:

Applicant mitigated the use of information technology security concerns, but he did not mitigate the personal conduct security concerns. Eligibility for access to classified information is denied.

## Statement of the Case

On July 2, 2016, the Department of Defense (DOD) issued a Statement of Reasons (SOR) to Applicant detailing security concerns under Guidelines E (personal conduct) and M (use of information technology). Applicant responded to the SOR on August 1, 2016, and requested a hearing before an administrative judge.

The case was assigned to me on January 18, 2017. The Defense Office of Hearings and Appeals (DOHA) issued a notice of hearing on February 27, 2017, scheduling the hearing for April 5, 2017. The hearing was convened as scheduled. Government Exhibits (GE) 1 through 3 were admitted in evidence without objection. Applicant testified, called two witness, and submitted Applicant's Exhibits (AE) A

through I, which were admitted without objection. DOHA received the hearing transcript (Tr.) on April 18, 2017.

## Findings of Fact

Applicant is a 58-year-old engineer employed by a defense contractor since 1999. He has held a security clearance for almost 30 years. He has a bachelor's degree. He has been married for more than 20 years. He does not have children.[1]

Applicant was traveling extensively for work in 2013, which placed a strain on his marriage. During a work trip in late 2013, he used his company laptop computer to access adult pornography. He used a flash drive that had a private browser, which he incorrectly believed would bypass the firewall and prevent his company from discovering his actions.[2]

Applicant was permitted to use the flash drive on the company computer, but he was not permitted to use the private browser that was on the drive. Viewing pornography on the company's computer was also against company policy. In about March 2014, he was suspended from work for one week without pay for his conduct. Applicant received therapy from January to April 2014. His counselor wrote that Applicant was "forthright, honest, and accountable in acknowledging his lack of judgment." Applicant expressed appropriate remorse for his conduct. He stated that he learned a valuable lesson and the conduct will not be repeated. His wife is aware of what happened.[3]

Applicant submitted a Questionnaire for National Security Positions (SF 86) in June 2014. Under Section 13A – Employment Activities, in regard to his current employment, Applicant answered "No" to the following question:

> For this employment, **in the last seven (7) years** have you received a written warning, been officially reprimanded, suspended, or disciplined for misconduct in the workplace, such as a violation of security policy?

Applicant also answered "No" to the use of information technology questions under Section 27, including the following:

> **In the last seven (7) years** have you introduced, removed, or used hardware, software, or media in connection with any information technology system without authorization, when specifically prohibited by rules, procedures, guidelines, or regulations, or attempted any of the above.

[1] Tr. at 33-35; GE 1; AE B, C, E.

[2] Tr. at 38-44, 75-83; Applicant's response to SOR; GE 2, 3.

[3] Tr. at 38-57, 75-83; Applicant's response to SOR; GE 2, 3; AE F.

Applicant was interviewed for his background investigation in April 2015. The interviewer asked Applicant to confirm, clarify, and discuss his responses to the SF 86. Applicant confirmed his negative response to the question under Section 13A that asked if he had been officially reprimanded, suspended, or disciplined for misconduct in the workplace. When confronted with his one-week suspension, Applicant admitted that he had been suspended for two violations of company policy: the use of the unauthorized device on the company laptop and viewing pornography on the laptop. When asked why he answered "No" to the question, Applicant responded that he could not recall why; that it was an oversight; and he may not have read the question correctly.[4]

Applicant denied intentionally providing false information on the SF 86. He stated in his response to the SOR that when he completed the SF 86, his "intention was to put the entire situation behind [him]." He wrote that he misinterpreted the questions to be limited to those situations involving classified information.

Applicant testified that he "rubberstamped" the SF 86, meaning that he simply copied the information from his previous SF 86, and he did not closely read the questions. He reiterated that he thought the questions were limited to punishment for mishandling classified information.[5]

I did not find Applicant's testimony credible. After considering all the evidence, including Applicant's age, education, experience, character evidence, and the clear wording of the questions, I find that Applicant intentionally falsified both of the relevant questions on the SF 86.

Two witnesses testified, and Applicant submitted documents and letters attesting to his excellent job performance, trustworthiness, honesty, professionalism, work ethic, leadership, dependability, loyalty, reliability, dedication, and integrity. Applicant is recommended for a security clearance.[6]

## Policies

This case is adjudicated under Executive Order (EO) 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 adjudicative guidelines (AG), which became effective on June 8, 2017.[7]

[4] GE 2.

[5] Tr. at 57-69, 83-88.

[6] Tr. at 11-32; AE A, D, G.

[7] The SOR was issued under the previous adjudicative guidelines. I have utilized the current adjudicative guidelines as required. However, my ultimate decision would be the same under either set of guidelines.

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 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(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."

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." 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 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 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

The security concern for use of information technology is set out in AG ¶ 39:

> 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.

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

> (e) unauthorized use of any information technology system.

Applicant knew he was violating company policy when he used a private browser on a flash drive to access adult pornography on his company laptop computer. The above disqualifying condition is applicable.

Conditions that could mitigate the use of information technology systems security concerns are provided under AG ¶ 41. The following is 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.

The conduct occurred in late 2013, almost four years ago. Applicant received therapy and expressed appropriate remorse for his conduct. He stated that he learned a valuable lesson and the conduct will not be repeated. AG ¶ 41(a) is applicable.

### Guideline E, Personal Conduct

The security concern for personal conduct is set out in AG ¶ 15, as follows:

> 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. Of special interest is any failure to cooperate or provide truthful and candid answers during national security clearance investigative or adjudicative processes.

AG ¶ 16 describes conditions that could raise a security concern and may be disqualifying. The following disqualifying condition is potentially applicable:

> (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.

Applicant intentionally falsified his SF 86 when he failed to report his suspension and his misuse of his company's computer. AG ¶ 16(a) is applicable.

AG ¶ 17 provides conditions that could mitigate security concerns. The following are potentially applicable:

> (a) the individual made prompt, good-faith efforts to correct the omission, concealment, or falsification before being confronted with the facts;
>
> (b) the refusal or failure to cooperate, omission, or concealment was caused or significantly contributed to by advice of legal counsel or of a person with professional responsibilities for advising or instructing the individual specifically concerning security processes. Upon being made aware of the requirement to cooperate or provide the information, the individual cooperated fully and truthfully;
>
> (c) the offense is so minor, or so much time has passed, or the behavior is so infrequent, or it happened under such unique circumstances that it is unlikely to recur and does not cast doubt on the individual's reliability, trustworthiness, or good judgment;
>
> (d) the individual has acknowledged the behavior and obtained counseling to change the behavior or taken other positive steps to alleviate the stressors, circumstances, or factors that contributed to untrustworthy, unreliable, or other inappropriate behavior, and such behavior is unlikely to recur; and
>
> (e) the individual has taken positive steps to reduce or eliminate vulnerability to exploitation, manipulation, or duress.

Having determined that Applicant intentionally provided false information on the SF 86, I have also determined that his explanations that the omission was unintentional were also false. It would be inconsistent to find that conduct mitigated.[8]

[8] *See* ISCR Case 03-22819 at 4 (App. Bd. Mar. 20, 2006), in which the Appeal Board reversed the Administrative Judge's decision to grant Applicant's security clearance:

> Once the Administrative Judge found that Applicant deliberately falsified a security clearance application in September 2002, the Judge could not render a favorable security

**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(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 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 the facts and circumstances surrounding this case. I have incorporated my comments under Guidelines E and M in my whole-person analysis. I considered Applicant's character evidence and his intentional violation of company policy. That conduct is mitigated. However, his intentionally false information about that conduct on his Questionnaire for National Security Positions is not mitigated.

Overall, the record evidence leaves me with questions and doubts as to Applicant's eligibility and suitability for a security clearance. I conclude Applicant mitigated the use of information technology security concerns, but he did not mitigate the personal conduct security concerns.

---

> clearance decision without articulating a rational basis for why it would be clearly consistent with the national interest to grant or continue a security clearance for Applicant despite the falsification. Here, the Judge gives reasons as to why he considers the falsification mitigated under a "whole person" analysis, namely that Applicant has matured, has held a position of responsibility, recognizes how important it is to be candid in relation to matters relating to her security clearance, and has changed her behavior so that there is little likelihood of recurrence. However, the Judge's conclusion runs contrary to the Judge's rejection of Applicant's explanations for the security clearance application falsification. At the hearing (after earlier admitting the falsification in her March 2003 written statement to a security investigator), Applicant testified that she had not intentionally falsified her application. Given the Judge's rejection of this explanation as not being credible, it follows that the Judge could not have concluded Applicant now recognizes the importance of candor and has changed her behavior.

## 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 |
| Subparagraphs 1.a-1.b: | For Applicant |
| Paragraph 2, Guideline E: | Against Applicant |
| Subparagraphs 2.a-2.b: | Against Applicant |

## Conclusion

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

_____
Edward W. Loughran
Administrative Judge