DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 19-01138
	)	
Applicant for Security Clearance	)	

Appearances

For Government: David F. Hayes, Esq., Department Counsel
For Applicant: Jeffrey D. Billet, Esq.

11/19/2019

_____

Decision

_____

LOUGHRAN, Edward W., Administrative Judge:

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

Statement of the Case

On May 24, 2019, 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 June 21, 2019, and requested a hearing before an administrative judge. The case was assigned to me on October 1, 2019. The hearing was convened as scheduled on October 30, 2019.

Evidence

Government Exhibits (GE) 1, 3, and 4 were admitted in evidence without objection. Applicant filed a motion in limine to exclude part of GE 2. The motion was denied, and GE 2 was admitted in evidence in its entirety. However, the part of GE 2 that was objected to has almost no probative value and is given the appropriate weight.

Applicant testified and submitted Applicant's Exhibits (AE) A through K, which were admitted without objection.

Findings of Fact

Applicant is a 40-year-old employee of a defense contractor. He has worked for his current employer (Company C) since 2018. He honorably served on active duty in the U.S. military from 1999 to 2003 and in the reserve from 2003 to 2006. He seeks to retain a security clearance, which he has held for an extended period. He has a bachelor's degree and additional credits but no post-graduate degree. He is single without children. (Transcript (Tr.) at 23-24, 28-31, 93-101; Applicant's response to SOR; GE 1, 2; AE A, C, D)

Applicant worked for a defense contractor (Company A) at different locations from 2013 until he was terminated in late October 2017. In August 2017, he was working overseas as a systems engineer on a U.S. defense project on an allied nation's military base. He was supposed to teach the foreign personnel how to use and troubleshoot the system. He stated that the foreign personnel were lax about security, and he became desensitized to it. In an attempt to fix the system, he violated security rules by logging into the system using the credentials of a member of the foreign country's military. (Tr. at 31-64, 73, 86-87, 111-132, 153; Applicant's response to SOR; GE 1, 2; AE A, J, K)

Applicant was questioned about the incident by members of the foreign country's military. He lied to them and denied that he used the foreign military member's credentials to log into the system. Applicant also lied orally and in writing to supervisory personnel from his employer. He later told the truth to an investigator from his employer. (Tr. at 64-85, 133-145; Applicant's response to SOR; GE 2-4; AE K)

Applicant admitted that he was initially untruthful to the foreign military and to his supervisors. He stated that he panicked when questioned by the military. He was alone in a room with four foreign military members, and he feared for his safety and freedom. He stated that he did not tell his supervisors the truth because he did not trust them. He stated that once he was questioned by the investigator he was completely forthcoming. (Tr. at 64-85, 133-145, 158; Applicant's response to SOR; AE K)

Applicant submitted a Questionnaire for National Security Positions (SF 86) in September 2017, while he was still employed by Company A. Under the employment section, he wrote that he was "warned, reprimanded, suspended, or disciplined" by Company A in September 2017, with the following description: "Logged in as another user to finish a task that I was assigned. An investigation was conducted with the results being that no information was taken and no malicious intent was done." (Tr. at 85; AE G)

Because of his actions in the foreign country, Applicant was terminated by Company A in late October 2017. He was hired by another defense contractor (Company B) in about November 2017. There was some difficulty in transferring his

clearance from Company A to Company B, and he was asked to complete another SF 86, which he submitted in December 2017. He was able to use the September 2017 SF 86 as a template and add anything that had to be updated. (Tr. at 73, 85-88, 145-147; GE 1; AE A, B)

Applicant reported his employment with Company A ended in November 2017. He repeated the same information from the previous questionnaire that he was "warned, reprimanded, suspended, or disciplined" by Company A in September 2017. He wrote the reason for leaving the job as "My position was downsized." (GE 1) He answered "No" to the following question:

> For this employment have any of the following happened to you **in the last seven (7) years?**
>
> - Fired
> - Quit after being told you would be fired
> - Left by mutual agreement following charges or allegations of misconduct
> - Left by mutual agreement following notice of unsatisfactory performance

Applicant was notified by Company B's facility security officer (FSO) on February 22, 2018, that his investigation was completed, and that based on an investigation dated May 2, 2013, he was "granted **Secret** eligibility" on January 24, 2018. (AE H)

Applicant requested a copy of his DOD Consolidated Adjudications Facility (CAF) adjudicative records on April 30, 2018. The DOD CAF replied on May 16, 2018, with a copy of the September 2017 SF 86. (AE G)

Applicant was interviewed for his background investigation in July 2018. A signed statement was not obtained, but the interview was summarized in a report of investigation (ROI). He voluntarily informed the investigator that he was terminated from Company A in October 2017. He told the investigator that he did not know why his questionnaire reported his position was downsized, as he completed the questionnaire in September 2017 while he was working for Company A. (Tr. at 90-91; GE 2; AE I)

Applicant was provided a copy of the ROI in DOHA interrogatories and asked about its accuracy. He wrote the following in a response, dated May 2, 2019: "I listed my position as downsized because my manager, [redacted], told me they were doing away with the position before I was terminated." (GE 2)

Applicant's response to the SOR was prepared by his attorney, but adopted by Applicant as the truth and notarized on June 21, 2019 (48 days after his response to DOHA interrogatories). The response stated:

> Regarding the CAF's allegation that [Applicant] submitted this SF 86 in December, and that he reported that he had been "downsized," he has not

been provided with any evidence that that is the case. He has no memory of that, has no reason to have lied when he had already been forthcoming about the same incident and later was forthcoming in an interview.

Applicant denied intentionally providing false information on the SF about his termination from Employer A. He stated that he submitted the September 2017 SF 86, but he did not remember submitting a second SF 86. He stated that he had no reason to lie because he reported the underlying conduct to the DOD. He asserted, without corroborating documentation, that Company B was aware that he had been terminated from Company A because he put it on his job application. He stated that he did not remember writing on the SF 86 that his position with Company A was "downsized," but if he did write it, it was because when he left the foreign country he was told by his supervisor that his position was being downsized and would be backfilled by a foreign national. (Tr. at 85-89, 108-111, 149-156; Applicant's response to SOR; GE 2)

Applicant volunteers in his community. He submitted documents and letters attesting to his excellent job performance in the military and as a civilian. He is praised for his moral character, honesty, patriotism, professionalism, trustworthiness, responsibility, work ethic, reliability, judgment, integrity, and willingness and ability to protect classified information. He is recommended for a security clearance. (AE B-F)

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.

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(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."

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 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 information. Of special interest is any failure to provide truthful and candid answers during the security clearance process or any other failure to cooperate with the security clearance process.

AG ¶ 16 describes conditions that could raise a security concern and may be disqualifying. The following disqualifying conditions are 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 security clearance eligibility or trustworthiness, or award fiduciary responsibilities;
>
> (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;

(c) credible adverse information in several adjudicative issue areas that is not sufficient for an adverse determination under any other single guideline, but which, when considered as a whole, supports a whole-person assessment of questionable judgment, untrustworthiness, unreliability, lack of candor, unwillingness to comply with rules and regulations, or other characteristics indicating that the individual may not properly safeguard classified or sensitive information; and

(e) personal conduct, or concealment of information about one's conduct, that creates a vulnerability to exploitation, manipulation, or duress by a foreign intelligence entity or other individual or group. Such conduct includes:

(1) engaging in activities which, if known, could affect the person's personal, professional, or community standing.

Applicant worked overseas as a systems engineer on a U.S. defense project on an allied nation's military base. He violated security rules by logging into the system using the credentials of a member of the foreign country's military. That conduct reflects questionable judgment and an unwillingness to comply with rules and regulations. It also created vulnerability to exploitation, manipulation, and duress. AG ¶¶ 16(c) and 16(e) are applicable.

Applicant was questioned about the incident by members of the foreign country's military. He lied to them and denied that he used the foreign military member's credentials to log into the system. He also lied to supervisory personnel from his employer. AG ¶ 16(b) is applicable.

Applicant submitted SF 86s in September 2017 (while he was still employed by Company A) and December 2017 (after he was terminated by Company A). He did not report on the December 2017 SF 86 that he was terminated by Company A. Instead, he wrote that his "position was downsized." He denied intentionally providing false information on the December 2017 SF 86. He stated that he had no reason to lie because he reported the underlying conduct to the DOD. He asserted that he did not remember completing the second SF 86, but if he did write that his position with Company A was "downsized," it was because when he left the foreign country he was told by his supervisor that his position was being downsized and would be backfilled by a foreign national.

I did not find Applicant credible, and I did not find his explanations to be worthy of belief. After considering all the evidence, including Applicant's testimony, age, education, experience, motive to fabricate, prior false statements, and strong character

evidence, I find by substantial evidence[1] that he intentionally provided false information about his termination from Company A on the December 2017 SF 86. 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.

Applicant admitted lying to the foreign military members and his employer's supervisors. He stated that he was intimidated by the foreign service members, and he did not trust his supervisors. He eventually told the truth to an investigator from his company. He was interviewed for his background investigation in July 2018. He voluntarily informed the investigator that he was terminated from Company A in October 2017.

Had Applicant been honest from the beginning about the circumstances surrounding his termination from Company A, that conduct would likely have been

[1] Substantial evidence is "such relevant evidence as a reasonable mind might accept as adequate to support a conclusion in light of all the contrary evidence in the same record." *See, e.g.,* ISCR Case No. 17-04166 at 3 (App. Bd. Mar. 21, 2019) (citing Directive ¶ E3.1.32.1). "This is something less than the weight of the evidence, and the possibility of drawing two inconsistent conclusions from the evidence does not prevent [a Judge's] finding from being supported by substantial evidence." *Consolo v. Federal Maritime Comm'n*, 383 U.S. 607, 620 (1966). "Substantial evidence" is "more than a scintilla but less than a preponderance." *See v. Washington Metro. Area Transit Auth*., 36 F.3d 375, 380 (4th Cir. 1994); ISCR Case No. 04-07187 at 5 (App. Bd. Nov. 17, 2006).

mitigated. However, Applicant has consistently denied that he lied on the December 2017 SF 86. Having determined that he intentionally omitted information from that SF 86, I have also determined that his explanations that the omissions were unintentional were also false. It would be inconsistent to find his conduct mitigated.[2] Without complete candor, there are no applicable mitigating conditions and none of the conduct is mitigated.

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 are potentially applicable:

> (a) unauthorized entry into any information technology system;
>
> (c) use of any information technology system to gain unauthorized access to another system or to a compartmented area within the same system; and
>
> (e) unauthorized use of any information technology system.

[2] *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 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.

Applicant violated security rules by logging into a system using the credentials of a member of the foreign country's military. The above disqualifying conditions are 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; and
>
> (b) the misuse was minor and done solely in the interest of organizational efficiency and effectiveness.

The above analysis under personal conduct also applies here. Applicant's conduct continues to cast doubt on his reliability, trustworthiness, and good judgment. AG ¶¶ 41(a) and 41(b) are not applicable.

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 have incorporated my comments under Guidelines E and M in my whole-person analysis. I also considered Applicant's honorable military service, his work overseas, and his strong character evidence, but the favorable information is insufficient to overcome his incidents involving questionable judgment and dishonesty.

Overall, the record evidence leaves me with questions and doubts about Applicant's eligibility and suitability for a security clearance. I conclude Applicant did not mitigate the personal conduct and use of information technology 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:	Against Applicant
Subparagraph 1.a:	Against Applicant
Paragraph 2, Guideline E:	Against Applicant
Subparagraphs 2.a-2.c:	Against Applicant

Conclusion

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