DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 18-02284
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Bryan J. Olmos, Esq., Department Counsel
For Applicant: *Pro se*

10/28/2019

_____

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 December 31, 2018, 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 March 25, 2019, and requested a hearing before an administrative judge. The case was assigned to me on June 24, 2019.

The hearing was convened as scheduled on August 9, 2019. Government Exhibits (GE) 1 through 3 were admitted in evidence over Applicant's objection. The objection to GE 4 was sustained. Applicant testified and submitted Applicant's Exhibits (AE) A and B, which were admitted without objection.

Findings of Fact

Applicant is a 61-year-old employee of a defense contractor. He has worked for his current employer for almost two years. He served in the National Guard from 1976 to 1977, and on active duty in the U.S. military from 1977 until he was honorably discharged in 1990. He seeks to retain a security clearance, which he has held for an extended period. He attended college, but he has not earned a degree. He is married for the second time. He has two children and a stepchild. (Transcript (Tr.) at 32-33; GE 1)

Applicant worked for a defense contractor at various locations for a number of years. In about February 2016, he was permitted to resign in lieu of termination after his employer discovered that he uploaded inappropriate materials onto the employer's computer system in violation of company policy. The uploaded materials included movies, television programs, and some materials that had sexually explicit content. The company also believed he mischarged his labor by viewing those materials on company time. (Tr. at 20, 24-32; Applicant's response to SOR; GE 1-3)

Applicant admitted that he resigned in lieu of termination, but he denied intentionally uploading sexually explicit materials. He asserted that his contract with the company was about to end, and he wanted to save some information for future use. He connected a personal external hard drive to the company's computer system and copied some information to the hard drive. He admitted that he listened to music and movies through the external hard drive while he worked the third shift. He denied watching movies while working. He asserted that his friends and co-workers uploaded the sexually explicit materials on the personal hard drive without his knowledge while he was working in Afghanistan, and that the materials must have been uploaded to the company's computer system by mistake. He also admitted that it was against company policy to connect a personal external hard drive to the company's computer system. (Tr. at 20, 24-32; Applicant's response to SOR; GE 2)

Applicant submitted a Questionnaire for National Security Positions (SF 86) in April 2017. Under Section 13A – Employment Activities, he reported the job discussed above that ended in February 2016. He intentionally provided false information when he wrote the reason for leaving the job as:

> Received a lay off letter in January 2016 from [Employer] and our jobs would be finished at end of February 2016. I had an opportunity early in Feb. 2016 to go and work with a different U.S. company overseas. They wanted me to go as soon as possible, so I resigned from [Employer] to take this job. But unfortunately someone else was picked for the position.

Applicant also intentionally provided false information on the SF 86 when 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 provided an additional false statement when he answered "No" to the following question under Section 27 – Use of Information Technology Systems:

> **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?

Applicant was interviewed for his background investigation in July 2018. He repeated the lie that he voluntarily resigned from his employer in February 2016 to pursue an opportunity overseas. When confronted with the facts about the resignation in lieu of termination, he continued his lie and stated that he did not commit any unfavorable conduct while working for the company. He denied misusing his employer's technology.

Applicant admitted at the hearing that he was untruthful on the SF 86 and to the background investigator. He stated that his former employer told him that if he resigned there would be no records of his being fired. (Tr. at 21-23, 35)

Applicant submitted documents and a letter attesting to his excellent job performance. He is praised for his technical knowledge and professionalism. (AE A)

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 intentionally provided false information about the circumstances surrounding his resignation in lieu of termination on an April 2017 SF 86 and during a background interview in July 2018. AG ¶¶ 16(a) and 16(b) are applicable.

Applicant violated his employer's policy when he connected a personal external hard drive to the company's computer. 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.

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 lied on the SF 86 and during his background interview. I have doubts that he was completely truthful at his hearing. Had he been honest from the beginning about the circumstances surrounding his resignation in lieu of termination, that conduct would likely have been mitigated. However, 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:

(e) unauthorized use of any information technology system; and

(f) introduction, removal, or duplication of hardware, firmware, software, or media to or from any information technology system when prohibited by rules, procedures, guidelines, or regulations or when otherwise not authorized.

Applicant knew he was violating company policy when he connected a personal external hard drive to the company's computer system. 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.

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) is 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 favorable character evidence.

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 E:	Against Applicant
Subparagraphs 1.a-1.d:	Against Applicant
Paragraph 2, Guideline M:	Against Applicant
Subparagraph 2.a:	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