DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 21-00239
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Brian Farrell, Esq., Department Counsel
For Applicant: *Pro se*

07/25/2022

_____

Decision

_____

DAM, Shari, Administrative Judge:

Applicant mitigated the use of information technology security concerns. Eligibility for access to classified information is granted.

Statement of the Case

On June 11, 2021, the Defense Counterintelligence and Security Agency (DCSA) issued a Statement of Reasons (SOR) to Applicant detailing security concerns under Guideline M (use of information technology). On July 6, 2021, Applicant answered the SOR, and requested a hearing before an administrative judge (Answer). The case was assigned to me on May 10, 2022.

On June 21, 2022, the Defense Office of Hearings and Appeals (DOHA) issued a notice of hearing, setting the hearing for July 13, 2022. The hearing was convened as scheduled. Department Counsel offered Government Exhibits (GE) 1 through 3 into evidence, which were admitted without objection. Applicant testified and offered Applicant Exhibits (AE) A through L, which were admitted without objection. I received the hearing transcript on August 9, 2022.

Findings of Fact

Applicant is 31 years old and married since 2018. He has two stepchildren and one child with his wife. He graduated from high school in June 2010. Immediately after graduating, Applicant enlisted in the Army for six years. He was stationed in a European country for a three-year tour. While there he deployed to the Middle East for eleven months on a combat mission. (Tr. 21-22 He served in the military until October 2016, when he was honorably discharged, as a logistical specialist (E-4). (Tr. 23) While serving, he received individual awards. (Tr. 23) He received his first security clearance in 2011 and has held it since then. (Tr. 59) He subsequently used his military benefits to earn a bachelor's degree in 2017 and a master's degree in 2021, both in the field of information technology. (Tr. 15-17, 23; GE 1 at 29.)

After his discharge from the Army, Applicant began working as a technical IT support representative for civilian company (FB) in August 2016. He worked there until April 2017 when he was fired for accessing his supervisor's email without authorization. (Tr. 19, 67; GE 1 at 24) Applicant admitted that he wrongly accessed said email and acknowledged that it was a mistake and childish behavior on his part. (Tr. 25, 31)

Applicant explained that FB was his first job after leaving active duty and he soon became frustrated with the company and the manner in which his supervisor treated employees. During his last work week at FB, (he had secured another position), he decided to access his supervisor's emails and review them for disparaging information about his co-workers. (Tr. 25, 28-29, 60) After locating some emails with pejorative statements, Applicant copied two excerpts and sent them in emails to his supervisor and the chief executive officer (CEO) on his last work day. In his email Applicant commented on their inappropriate conduct involving employees. (Tr. 32, 45-46) Applicant said this was the only time he accessed his supervisor's email (Tr. 27, 32) He has never accessed anyone else's email since this incident. (Tr. 34, 39, 47)

In retrospect, Applicant admitted that his behavior was impulsive and unprofessional. He acknowledged that he was upset with the FB's treatment of employees. He agreed that he should have handled his concerns differently, such as by talking to his supervisor instead of accessing his email. (Tr. 62, 67)

After leaving FB in April 2017, Applicant started working for civilian IT company HC. In June 2017, he was fired for accessing a company's application without having proper credentials while he was on a 90-day probation. Applicant explained that his supervisor assigned him a task for which he needed access to a specific system in order to perform the work. Thinking that she wanted the work completed, he asked his co-worker for the organization's login credentials. He did not ask for the co-worker's personal information. He said his co-worker provided the company's login and he then completed the task and logged out. The following day, another supervisor discovered his actions and fired him. (Tr. 50)

Applicant said he did not make any mistakes in completing the task, but was fired because he was in the probationary period and did not yet have access to that system.

(Tr. 56) He does not think that his co-worker who provided the information was disciplined for giving him the information. (Tr. 52) He acknowledged that he should have clarified his supervisor's request before asking his co-worker for the company's login credentials. (Tr. 51)

In July 2017, Applicant started working for civilian company A, as a software analyst. He left that position in October 2018 for a better paying position with government contractor D. He worked for D for two months as a systems administrator, at which time the contract ended. He then started a position with the Army in January 2019 and stayed there until July 2019, when that contract ended. (GE 1 at 18-25) In August 2019, he began his current position with defense contractor (K), as a senior system administrator and site lead. This position requires a security clearance. (Tr. 14)

On April 27, 2021, the CEO for FB signed an affidavit regarding Applicant's termination with FB in August 2016. In it, the CEO stated Applicant disseminated information to employees about management activities, meetings, salary, and performance information. (AE 3) Applicant denied that allegation and said he never saw that information and did not have access to it. (Tr. 43-44)

Applicant testified that he has not had any employment issues since leaving HC, in June 2017. He has never accessed another person's email, used a logon password that was not his, or been disciplined for wrongdoing. He said he has received excellent reviews at K. (Tr. 56-58). He told all of the people who submitted character references about his past conduct, as well as his wife. (Tr. 63-64) He admitted that he held a position of trust at FB and violated it by accessing his supervisor's email. (Tr. 66)

Applicant submitted nine letters attesting to his excellent job performance and strong moral character. One of the letters is from a soldier with whom he served. The other eight letters are from colleagues with whom he has worked since early 2019. He is praised for his trustworthiness, work ethic, and judgment. (AE D through AE L) The contracting officer for the project Applicant works on wrote that she has known him since January 2019. She stated he is a critical part of her team and he supervises 11 employees." (AE D) She said he is "exceptionally trustworthy." (*Id.*) A senior systems administrator started working closely with Applicant when he arrived in 2019. He stated that Applicant "possesses a great deal of integrity and constantly strives to make sure he is doing the right thing." (AE J)

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 M: Use of Information Technology

The security concerns relating to the guideline for use of information technology are 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.

The guideline notes conditions that could raise security concerns under AG ¶ 40. The following three are potentially applicable in this case:

> (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.

Applicant admitted that he accessed his supervisor's company e-mail, one time, in April 2017, while working at company FB. He admitted that he used another employee's credentials at company HC to gain access to a program that he was unauthorized to use because he was on probation in June 2017. He was terminated from both companies as a consequence of his actions. The evidence raised disqualifying conditions under AG ¶¶ 40(a), 40(c) and 40(e) as to SOR ¶ 1.a and SOR ¶ 1.c.

Applicant denied that while he worked at company FB, he accessed specific types of company information from his supervisor's email and forwarded it to employees, as alleged in SOR ¶ 1.b. No documents were produced verifying the CEO's assertion, which is the basis for the allegation. There is insufficient evidence to establish a disqualifying condition under AG ¶ 40 as to that SOR allegation. SOR ¶ 1.b is found in Applicant's favor.

Conditions that could mitigate the above use of information technology 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.

Over the past five years, Applicant has not been warned or disciplined for misusing his position or accessing his employer's information technology. More importantly, he acknowledges his wrongdoing and takes responsibility for it. Similar incidents are unlikely to recur given Applicant's appreciation of the consequences he encountered after being fired from two positions, which have subsequently jeopardized his security clearance. Eight current colleagues, who have known him since early 2019 and one prior to that date, attest to his over-all trustworthiness, reliability, and diligence in complying with IT rules. The evidence establishes mitigation for the allegations in SOR ¶ 1.a and SOR ¶ 1.c.

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 facts and circumstances surrounding this case. I have incorporated my comments under Guideline M in my whole-person analysis. I have also considered the following facts: Applicant's military service, his remorse over his misconduct in 2017, the absence of subsequent incidents, his favorable character evidence from current colleagues, and his statement that he told those colleagues about his misconduct, as well as his wife. His disclosures to those people diminish the potential for coercion or exploitation and the likelihood of recurrence.

Overall, the record evidence leaves me without questions or doubts about Applicant's eligibility and suitability for a security clearance. Applicant mitigated the 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:	For Applicant
Subparagraph 1.a:	For Applicant
Subparagraph 1.b:	For Applicant
Subparagraph 1.c:	For Applicant

Conclusion

It is clearly consistent with the national interest to grant Applicant eligibility for a security clearance. Eligibility for access to classified information is granted.

_____
Shari Dam
Administrative Judge