DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 18-00766
	)	
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Andrew C. Henderson, Esq., Department Counsel
For Applicant: *Pro se*

March 6, 2019

_____

Decision

_____

Lokey Anderson, Darlene D., Administrative Judge:

Statement of the Case

On May 11, 2018, 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 Guideline K. The SOR further informed Applicant that, based on information available to the government, DoD adjudicators could not make the preliminary affirmative finding it is clearly consistent with the national interest to grant or continue Applicant's security clearance.

Applicant answered the SOR on May 29, 2018, and requested a hearing before an administrative judge. (Answer.) The case was assigned to me on September 5, 2018. The Defense Office of Hearings and Appeals (DOHA) issued a notice of hearing on November 15, 2018, scheduling the hearing for December 4, 2018. The hearing was convened as scheduled. The Government offered Exhibits Government Exhibits 1 through 5, which were admitted without objection. Applicant testified on his own behalf and presented five documents, which I marked Applicant's Exhibits A through E. DOHA received the transcript of the hearing (TR) on December 13, 2018.

Findings of Fact

Applicant admitted to the allegations in the SOR under this guideline. After a thorough and careful review of the pleadings, exhibits, and testimony, I make the following findings of fact.

Applicant is 36 years old. He is married, and has one minor son. He has a Master's degree in Systems Engineering. He holds the position of System Test Engineer for a defense contractor.

Applicant was born in Vietnam in 1981. He immigrated to the United States in 1995 with his father and younger brother. Applicant became a naturalized U.S. citizen in 2003. (Tr. p. 22.) He graduated from college with his bachelor's degree in 2006, and received his Master's degree in 2012. He has been employed with his current employer, a defense contractor, since 2008 and has held a security clearance since then. Applicant testified that since obtaining his security clearance, he has received annual security briefings from his employer as a refresher. (Tr. p. 23.)

While working for his current employer, since 2008, Applicant has committed three security violations and/or infractions occurring in 2014, 2016, and 2017. The first one occurred in September 2014. On this occasion, Applicant left classified information unattended in violation of his company's security regulations. Applicant explained that he had been working late, writing what he calls a test procedure, in a classified room within a safe lab, known as a secret area, when he wrote several numbers down on a piece of paper. (Tr. p. 24-25.) He left the piece of paper on the table. Another individual came in the following morning and found the piece of paper with the numbers on it and reported it to company security department. While conducting their investigation, they determined that no one had accessed the area since Applicant left. (Tr. p. 26.) Following this security infraction, Applicant was interviewed by the security department and he was required to provide a written statement about the incident and received a security infraction that was placed in his company personnel file. He was also required to take and complete the annual security training immediately after the incident. (Tr. p 27.)

The second security violation occurred in November 2016. Applicant stated that he was the response engineer for a test procedure in an unclassified program document. He had been working on the document for some time and had made several revisions, updates to the procedures, and put numbers to the procedure. At some point, it was discovered by the customer that Applicant had included classified information in the document. (Tr. p. 29.) The customer sent it to their security department, and it was determined to be a Code Blue, where there was a mass data containment effort. Industrial security investigators later confirmed that the classified information in the program document was compromised. Following this security violation, Applicant was interviewed by the security department and was required to provide a written statement about the incident, and he received a security violation that was placed his company's personnel file. Once again, he was required to take and complete the annual security training.

Applicant's third security violation occurred in or about April 2017. This time, Applicant did not properly check to ensure that the classified safe was properly closed. Applicant explained that he signed an acknowledgment form attesting to the fact that he witnessed his supervisor properly secure a safe holding classified documents. The company security department conducted a daily scan and discovered that they were able to open the safe, and that it had not been properly secured in violation of company security regulations. Applicant later realized that he had not pulled down the handle to ensure that it could was properly secured. Following this security violation, Applicant was interviewed by the security department and was required to provide a written statement about the incident. He received a security violation that was placed his company's personnel file. Once again, he was required to take and complete the annual security training.

Applicant states that he was never disciplined for any of the three security infractions/violations. He believes that the first two incidents occurred because he did not understand the information enough to know that it was considered classified. The third violation he admits occurred because he simply missed it and made a mistake. (Tr. p. 40.)

Performance evaluations of the Applicant for 2015, 2016, and 2017, are favorable and reflect that he is a "Top Performer." (Applicant's Exhibit A.)

Five letters of recommendation from fellow colleagues and upper management who know and work with the Applicant, namely a Senior Computer Engineer and coworker, a Program Director, an Engineering fellow, and Applicant's current supervisor, each reflect that they believe Applicant is a dedicated individual who demonstrates a high level of technical capability, integrity, honesty and trustworthiness. Applicant is recommended for a security clearance. (Applicant's Exhibits B, C, D, and E.)

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 useful 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 AG ¶ 2 describing 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." In reaching this decision, I have drawn only those conclusions that are reasonable, logical and based on the evidence contained in the record. Likewise, I have avoided drawing inferences grounded on mere speculation or conjecture.

Under Directive ¶ E3.1.14, the Government must present evidence to establish controverted facts alleged in the SOR. Under Directive ¶ E3.1.15, an "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 Executive Order 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 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 handling protected information-which includes classified and other sensitive government information, and proprietary information-raises doubt about an individual's trustworthiness, judgment, reliability, or willingness and ability to safeguard such information, and is a serious security concern.

The guideline notes nine conditions that could raise security concerns under AG ¶ 34. Five are potentially applicable in this case:

> (a) deliberate or negligent disclosure of protected information to unauthorized persons, including, but not limited to, personal or business contacts, the media, or persons present at seminars, meetings, or conferences;
>
> (b) collecting or storing protected information in any unauthorized location;
>
> (g) any failure to comply with rules for the protection of classified or sensitive information;
>
> (h) negligence or lax security practices that persist despite counseling by management; and
>
> (i) failure to comply with rules or regulations that results in damage to the national security, regardless of whether it was deliberate or negligent.

AG ¶ 35 provides conditions that could mitigate security concerns. I considered all of the mitigating conditions under AG ¶ 35 including:

> (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;
>
> (b) the individual responded favorably to counseling or remedial security training and now demonstrates a positive attitude toward the discharge of security responsibilities;
>
> (c) the security violations were due to improper or inadequate training or unclear instructions; and
>
> (d) the violation was inadvertent, it was promptly reported, there is no evidence of compromise, and it does not suggest a pattern.

None of the mitigating conditions are applicable. As a holder of a security clearance and entrusted with working with the Government's classified information, Applicant had a duty to be responsible, careful, and vigilant while protecting classified information. In this situation, clearly he was not. Applicant states that he was not clear regarding certain rules and regulations that pertain to classified information. So although he did not deliberately intend to commit two of the three security infractions/violations, he was negligent and careless. He did not go to his company for clarification of the rules, nor did he seek out any other assistance before committing the security violations. This does not show good judgment.

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 national security eligibility 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 K, in my whole-person analysis. Some of the factors in AG ¶ 2(d) were addressed under those guidelines, but some warrant additional comment. It is noted that Applicant has received favorable evaluations on the job, and is respected by his colleagues.

Overall, the record evidence leaves me with questions and doubts as to Applicant's eligibility and suitability for a security clearance. For all these reasons, I conclude Applicant failed to mitigate the Handling Protected Information security concerns.

Formal Findings

Formal findings for or against Applicant on the allegations set forth in the SOR, as required by ¶ E3.1.25 of the Directive, are:

Paragraph 1, Guideline K:	AGAINST APPLICANT
Subparagraph 1.a:	Against Applicant
Subparagraph 1.b:	Against Applicant
Subparagraph 1.c:	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 grant Applicant eligibility for a security clearance. National security eligibility for access to classified information is denied.

Darlene Lokey Anderson
Administrative Judge