



DEPARTMENT OF DEFENSE  
DEFENSE OFFICE OF HEARINGS AND APPEALS



In the matter of: )  
)  
) ISCR Case No. 19-00110  
)  
Applicant for Security Clearance )

**Appearances**

For Government: Ross Hyams, Esq., Department Counsel  
For Applicant: *Pro Se*

02/11/2021

---

**Decision**

---

GARCIA, Candace Le'i, Administrative Judge:

Applicant mitigated the security concerns related to handling protected information and personal conduct. Eligibility for access to classified information is granted.

**Statement of the Case**

On June 7, 2019, the Department of Defense (DOD) issued Applicant a Statement of Reasons (SOR) detailing security concerns under Guideline K (handling protected information) and Guideline E (personal conduct). The action was taken under Executive Order (Exec. Or.) 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) implemented by DOD on June 8, 2017.

Applicant responded to the SOR (Answer) on July 26, 2019 and requested a hearing before an administrative judge. The case was assigned to me on February 21, 2020. The Defense Office of Hearings and Appeals (DOHA) issued a notice of hearing (NOH) on March 10, 2020, scheduling the hearing for April 2, 2020. DOHA canceled the

hearing on March 19, 2020, due to DOD restrictions resulting from COVID-19. DOHA issued another NOH on June 29, 2020, rescheduling the hearing for July 17, 2020. I convened the hearing as rescheduled. (Tr. at 10-11)

Government Exhibits (GE) 1 through 3 and Applicant Exhibit (AE) A were admitted in evidence without objection. Applicant testified. She did not call any witnesses. At Applicant's request, I kept the record open until August 3, 2020. By that date, Applicant submitted documentation which I collectively marked as Applicant's Exhibit (AE) B and admitted in evidence without objection. DOHA received the hearing transcript (Tr.) on July 29, 2020. (Tr. at 11, 19-23, 77-80)

### **Findings of Fact**

Applicant admitted the allegation in SOR ¶ 2.b and denied the allegations in SOR ¶¶ 1.a, 1.b, and 2.a. Her admissions are incorporated in my findings of fact. (Answer; Tr. at 12-15; GE 1)

Applicant is 26 years old. She graduated from high school in 2012. She attended some college but had not yet earned a degree. She previously worked for three DOD contractors between approximately 2014 and 2017. As of the date of the hearing, she worked in accounting for a private company. She has never held a security clearance. Her offer of employment from another DOD contractor was contingent on obtaining a clearance. (Tr. at 7-10, 30-33; GE 1, 2)

The SOR alleges that Applicant failed to follow required security procedures for the protection of classified information in April 2017, when she allowed an unauthorized individual: (1) access to a secure building, (2) access behind the security desk through a security bypass door, and (3) use of a secure computer terminal in direct violation of client contract requirements (SOR ¶¶ 1.a, 1.b). The SOR also alleges that she was terminated for cause from her employment as a security officer in April 2017, after allowing the above-mentioned unauthorized individual use of a secure computer terminal (SOR ¶ 2.a). The SOR also alleges that she was terminated from employment in August 2017, as a security officer with another employer, for improper conduct (SOR ¶ 2.b).

Applicant first became a security officer in approximately 2015, at age 21. She worked as a "floater" and was assigned to various sites as needed. In April 2017, at age 23, she worked at a site for which she had just been assigned two months prior. She had just completed training. While assisting an employee, another individual approached the security bypass door and informed Applicant that she needed a replacement badge. Applicant obtained the individual's identification card and verified on the computer system that the individual was an employee. Applicant then obtained approval, from another experienced security officer on duty, to escort the individual through the security bypass door and to the security desk so that Applicant could issue the individual a badge. When Applicant tried to further verify the individual's credentials on the computer system, Applicant repeatedly mistyped the individual's name. When the individual offered to help, Applicant placed the keyboard on the upper level of the security desk to allow the individual to type in her own information. Applicant acknowledged that she should not

have done this. Upon locating the individual's credentials, the individual subsequently began to walk behind the security desk so that she could see the information on Applicant's computer screen. Applicant told her to stop, at which point the individual returned to the front of the security desk. Applicant then proceeded with issuing the individual her badge. (Tr. at 24-44, 51-64, 66-77; GE 1-3; AE A)

When Applicant reported to work the following day, two on-duty security officers told her that she no longer worked there. She did not receive a response when she texted her supervisor to ask what was going on. After several days, she reported to the office as instructed and was informed that she was terminated. Employment records reflect that she was discharged for allowing an authorized individual use of a secure computer. She denied responding, "No big deal." She testified that she believed she did primarily as she was trained, but acknowledged her poor judgment in permitting the unauthorized individual to use her computer keyboard. (Tr. at 24-44, 51-64, 66-77; GE 1-3; AE A)

Applicant acknowledged that she had previous unfavorable incidents with the same employer. In February 2016, she was given a written warning for violating her employer's phone policy when she pulled out her phone while on duty. In April 2016, she was given a written warning for tardiness. In June 2016, she was given a final warning for abandoning her post after she could not find the device she needed to patrol the site. She testified that she did so only after she unsuccessfully attempted to contact her supervisor multiple times and consequently believed that her employer no longer had authority over the site. In July 2016, she was verbally reprimanded for poor attendance. In January 2017, she was verbally reprimanded for violating her employer's uniform policy when she was not in proper uniform while on duty. She testified that she understood the importance of following her employer's rules and regulations, even if she found them to be strict. (Tr. at 17, 27-29, 31, 44-64, 66-77; GE 1-3)

After working for another DOD contractor for approximately two months, Applicant was terminated from employment as a security officer in August 2017, due to improper conduct. She testified that she reported to work approximately 30 minutes late because she had to change her car's flat tire in the rain. She called her manager and her on-site co-worker to report her tardiness. She was drenched upon arriving at work so she wrung out her uniform and took off her shoes and socks in an effort to get dry. Her actions were captured on camera and her supervisor notified her the following day that she was dismissed due to a consequent client complaint. She testified that she understood that she should have handled her discomfort privately. She has not since had any other unfavorable incidents with other employers and testified that she has matured and learned from her mistakes. (Tr. at 28-31, 64-77; GE 1-2)

Applicant's character references, to include her current employer, a former colleague, and two friends, describe her as a responsible and trustworthy individual. (AE B)

## Policies

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 Exec. Or. 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* Exec. Or. 12968, Section 3.1(b) (listing multiple prerequisites for access to classified or sensitive information).

## Analysis

### Guideline K, Handling Protected Information

The security concern 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 the conditions that could raise security concerns under AG ¶ 34. I have considered all of the disqualifying conditions under ¶ AG 34 and considered the following relevant:

(g) any failure to comply with rules for the protection of classified or sensitive information; and

(h) negligence or lax security practices that persist despite counseling by management.

Applicant failed to exercise good judgment and demonstrated negligent and lax security practices as a security officer from 2016 to 2017. She received multiple verbal and written warnings for violating her employer's phone, uniform, and attendance policies, and for abandoning her post. One employer discharged her after she allowed an unauthorized individual use of her secure computer, and another did so after she violated that employer's uniform policy. AG ¶¶ 34(g) and 34(h) are established.

Conditions that could mitigate the security concerns involving handling protected information are provided under AG ¶ 35. I have considered all of the mitigating conditions under ¶ AG 35 and considered the following relevant:

(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.

Applicant was young and a new security officer in 2016 and 2017. She accepted responsibility for her failure to comply with rules for the protection of classified or sensitive information and her negligent and lax security practices. She has learned from them. She has not since had any other unfavorable incidents with subsequent employers. I find that AG ¶ 35(a) is established.

### **Guideline E, Personal Conduct**

The personal conduct security concern is set out in AG ¶ 15:

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 investigative or adjudicative processes. . . .

AG ¶ 16 describes conditions that could raise a security concern and may be disqualifying. I have considered all of the disqualifying conditions under AG ¶ 16 and considered the following relevant:

(d) credible adverse information that is not explicitly covered under any other guideline and may not be sufficient by itself for an adverse determination, but which, when combined with all available information, 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. This includes, but is not limited to, consideration of:

(1) untrustworthy or unreliable behavior to include breach of client confidentiality, release of proprietary information, unauthorized release of sensitive corporate or government protected information; and

(3) a pattern of dishonesty or rule violations.

For the same reasons as set forth above under my Guideline K analysis, AG ¶¶ 16(d)(1) and 16(d)(3) are established.

I have considered all of the mitigating conditions under AG ¶ 17 and considered the following relevant:

(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; and

(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.

Also for the same reasons as set forth above, I find that AG ¶¶ 17(c) and 17(d) are established.

### **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 K and E in my whole-person analysis. Overall, the record evidence leaves me without questions or doubts as to Applicant's eligibility and suitability for a security clearance. I conclude Applicant mitigated the security concerns involving handling protected information and personal conduct.

### **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 K:	FOR APPLICANT
Subparagraphs 1.a - 1.b:	For Applicant
Paragraph 2, Guideline E:	FOR APPLICANT
Subparagraphs 2.a - 2.b:	For Applicant

### **Conclusion**

In light of all of the circumstances presented by the record in this case, it is clearly consistent with the national interest to grant Applicant's eligibility for a security clearance. Eligibility for access to classified information is granted.

---

Candace Le'i Garcia  
Administrative Judge