



**DEPARTMENT OF DEFENSE  
DEFENSE OFFICE OF HEARINGS AND APPEALS**

In the matter of: )  
)  
) ISCR Case No. 18-01313  
)  
Applicant for Security Clearance )

**Appearances**

For Government: Alison O’Connell, Esq., Department Counsel  
For Applicant: Krista Wallace, Esq.

05/22/2019

**Decision**

Curry, Marc E., Administrative Judge:

The allegations against Applicant were unsubstantiated. Clearance is granted.

**Statement of the Case**

On August 22, 2018, the Department of Defense Consolidated Adjudications Facility (DOD CAF) issued a Statement of Reasons (SOR) to Applicant, detailing the security concerns under Guideline K, handling protected information, and Guideline E, personal conduct, explaining why it was unable to find it clearly consistent with the national interest to grant security clearance eligibility. The DOD CAF took the action under Executive Order (EO) 10865, *Safeguarding Classified Information within Industry* (February 20, 1960), as amended; and DOD Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (January 2, 1992), as amended (Directive) and the National Security Adjudicative Guidelines (AG), effective June 8, 2017.

In an undated answer, Applicant denied the allegations and requested a hearing. On November 21, 2018, Department Counsel amended the SOR , adding a paragraph, alleging Guideline E, personal conduct, amending subparagraph 1.b by making it subparagraph 2.a, and cross-alleging 1.a as subparagraph 2.b to include the alleged

misconduct under the personal conduct guideline.

On January 16, 2019, the case was assigned to me, after having been transferred from another administrative judge. On February 12, 2019, the Defense Office of Hearings and Appeals issued a notice of hearing, scheduling Applicant's case for March 11, 2019. The hearing was held as scheduled. I received four Government exhibits (GE 1 – GE 4), four Applicant exhibits (AE A - AE D), and a copy of the discovery letter from Department Counsel to Applicant, dated November 21, 2018. Also, I considered the testimony of Applicant and three character witnesses. Another witness who was at the hearing and prepared to testify had to leave early, prompting Applicant's counsel to request that the record be kept open for a week to submit a character letter. Department Counsel did not object, and I left the record open. Within the time allotted, Applicant's counsel submitted a reference letter from the witness who had to leave the hearing early, and I incorporated the letter into the record as AE E. The transcript was received on March 27, 2019.

### **Findings of Fact**

Applicant is a 58-year-old single woman. Since 2012, she has worked as a security assistant for various federal contractors. (GE 1 at 9-24) According to her current supervisor, with whom she has worked since July 2016, she is a conscientious worker who comes to work on time and on a regular basis. Moreover, her integrity is "beyond reproach," and she has the strongest work ethic of any of his subordinates. (Tr. 52-53) A former coworker characterized Applicant as "a very professional, funny, caring, and conscious professional," who was well-liked by the team, and who always ensured that each member of the team participated in each team-building activity. (Answer at 6) Another coworker, who worked with Applicant from approximately July 2016 to July 2018, characterized her as "dependable, real self-motivated, and loyal." (Tr. 60)

Applicant was granted a security clearance in 2012. (GE 1 at 41) It was suspended in 2016, pending the outcome of this security clearance decision. (GE 3 at 2)

SOR subparagraph 1.a alleges that in December 2015, during an interview with a panel of employees from a contracting firm, Applicant disclosed that she kept access code combinations written down on a piece of paper in her possession while working for her then-employer, between October and November 2015, and that she verbally disclosed access code combinations. Applicant acknowledges that she underwent an interview in December 2015, and that she discussed the security procedure for opening the Sensitive Compartmented Information Facility (SCIF) where she was then working. (Tr. 24) However, she denies that she either failed to follow security procedures when she worked in the SCIF, or that she disclosed access combinations during the interview. Specifically, she testified that the SCIF where she worked could be entered with security cards. Before the security cards could operate, the agency's security specialist,<sup>1</sup> as the first person who arrived each morning, had to open it by unlocking each of the three successive doors that led to the SCIF. (Tr. 37) After this task was performed, the SCIF was accessible by security cards for the remainder of the day. (Tr. 39-40)

---

<sup>1</sup> Applicant was working onsite at a federal government agency. (Answer at 7)

One day, the security specialist asked Applicant to open the SCIF the following morning. He issued Applicant the code to a secured cabinet, which Applicant used to open the cabinet lock and retrieve an envelope with three combinations enclosed for the successive doors. (Tr. 25) To aid her memory, Applicant wrote the combinations to the successive doors on a sheet of paper. (GE 4 at 3) After opening each successive door and getting to her desk, which was located in the SCIF, she tore up the paper and placed it in her burn bag. (Tr. 46) The paper that contained the combinations was never out of Applicant's possession when she was referring to it to open the combinations. (Tr. 25)

Applicant never performed morning SCIF-opening duty again. (Tr. 25) There is conflicting record information concerning whether writing down security access codes constituted a security infraction. She contends that writing down the codes for the security doors, then tearing them up and disposing them in a burn bag was not a security infraction. (Tr. 32) A character witness testified that it constituted a security infraction to write down a combination to a classified cabinet. (Tr. 67) There is no record evidence of a company rule or procedure that addresses this issue.

SOR subparagraph 1.b alleges that Applicant told the interview panel at the December 2015 interview, that she hears voices in her head. Applicant denies this allegation. (Answer; Tr. 29) She has never heard imaginary voices or been diagnosed with a psychiatric condition, nor has she ever sought treatment or been hospitalized for a psychiatric condition. (Tr. 29) After Applicant learned of the allegation set forth in subparagraph 1.b, she contacted the head of the panel that interviewed her in 2015. The panel chairwoman denied making this allegation. (GE 4 at 3)

Applicant has been receiving medical services from a primary care provider since 2012. (Tr. 30) According to a nurse practitioner from the practice, Applicant is not being treated for any psychiatric conditions. (AE D) Per a friend who has known Applicant for 20 years, she has never displayed any symptoms of a psychiatric condition. (Tr. 57) Similarly, a coworker who worked with Applicant in 2012 noticed no symptoms indicative of a psychiatric condition. (Tr. 64)

The allegations that form the basis of the SOR were reported to the Defense Security Service (DSS) by the facility security officer of the company where Applicant interviewed, on December 21, 2015, three days after the interview occurred. (GE 3) On March 15, 2016, DSS suspended Applicant's security clearance. (GE 3 at 2)

The DSS report does not identify the individuals who made the adverse statements. It also incorrectly states Applicant's place of employment at the time of the interview. (Tr. 19)

## Policies

The U.S. Supreme Court has recognized the substantial discretion the Executive Branch has in regulating access to information pertaining to national security, emphasizing that “no one has a ‘right’ to a security clearance.” *Department of the Navy v. Egan*, 484 U.S. 518, 528 (1988). 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 required to be considered 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, these guidelines are applied together with the factors listed in the adjudicative process. The administrative judge’s overall 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.” In reaching this decision, I have drawn only those conclusions that are reasonable, logical, and based on the evidence contained in the record. 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 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 that the applicant may deliberately or inadvertently fail to safeguard classified information. Such decisions entail a certain degree of legally permissible extrapolation about potential, rather than actual, risk of compromise of classified information. Section 7 of Executive Order 10865 provides that 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).

Under the whole-person concept, the administrative judge must consider the totality of an applicant’s conduct and all relevant circumstances in light of the nine adjudicative process factors in AG ¶ 2(d).<sup>2</sup>

---

<sup>2</sup> The factors under AG ¶ 2(a) are as follows:

## Analysis

### Guideline K: Handling Protected Information

The security concerns about handing protected information are set forth in AG ¶ 13:

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.

Applicant wrote access code combinations on a piece of paper, which she used to aid her memory, as she opened three doors to a SCIF, on one occasion seven years ago, while working for a former employer. Her recollection of whether writing down a combination to a classified safe constitutes a security infraction conflicted with the recollection of a former coworker, who testified that such conduct would constitute a security infraction. However, there is no record evidence of an express company rule or procedure rule prohibiting this conduct. Absent record evidence of such a rule or procedure, I conclude that Applicant’s conduct does not constitute a mishandling of protected information. Assuming, for the sake of argument, that Applicant’s conduct constituted a security infraction, triggering AG ¶ 34(g),<sup>3</sup> the length of time since it elapsed, and its isolated nature, trigger the application of AG ¶ 35(a).<sup>4</sup>

The allegation that Applicant disclosed the access codes at an interview is based on GE 2, a DSS Suspicious Contact Report. No one is identified in the report. The probative value of the report is further limited as it contains the wrong city for where Applicant was working when the 2012 episode with the security access codes occurred. Upon weighing this report against Applicant’s denial and the positive record evidence of her integrity – particularly, the character reference of her current supervisor - I conclude that the allegation that Applicant disclosed the access codes at her interview is unsubstantiated. In sum, I conclude that there are no Guideline K security concerns.

---

(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.

<sup>3</sup> Any failure to comply with rules for the protection of classified or sensitive information.

<sup>4</sup> 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.

## **Guideline E, Personal Conduct**

Under this guideline, “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.” (AG ¶ 15) Applicant’s conduct, as cross-alleged in SOR subparagraphs 1.a and 2.b, was unsubstantiated. Consequently, it generates no security concern under either the guideline governing the mishandling of protected information, or the personal conduct guideline.

The allegation that Applicant hears imaginary voices, if true, would trigger the application of AG ¶ 16(d)(1), “untrustworthy or unreliable behavior . . .”, and AG ¶ 16(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.” Applicant denies this allegation. The credibility of her denial is bolstered by the record evidence of her good job performance and strong character.

The allegation that Applicant disclosed hearing imaginary voices to an interview panel is encapsulated in a DSS report that neither identifies the members of the interview panel, nor indicates which of the members of the interview panel made the allegation. The only member of the interview panel identified in the record denied making this allegation when contacted by Applicant. The DSS report also misstates Applicant’s place of employment when the interview occurred. Upon weighing this adverse information report against the positive record evidence, I conclude that the SOR allegations contained within it are unsubstantiated. There are no personal conduct security concerns.

## **Whole-Person Concept**

In weighing Applicant’s credibility, I considered her strong work ethic, sterling reputation, and integrity.

## **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
Subparagraph 1.a:	For Applicant
Subparagraph 1.b:	WITHDRAWN
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 interests of national security to grant Applicant eligibility for a security clearance. Eligibility for access to classified information is granted.

---

Marc E. Curry  
Administrative Judge