



**DEFENSE LEGAL SERVICES AGENCY
DEFENSE OFFICE OF HEARINGS AND APPEALS**



In the matter of:

Applicant for Security Clearance

)
)
)
)
)

ISCR Case No. 24-02477

Appearances

For Government: John Renehan, Esq., Department Counsel

For Applicant: *Pro se*

06/11/2026

Decision

ROSS, Wilford H., Administrative Judge:

Applicant did mitigate the security concerns arising from his past failure to comply with rules and regulations for handling protected information and related personal conduct. Eligibility for access to classified information is granted.

Statement of the Case

On May 12, 2025, the Defense Counterintelligence and Security Agency (DCSA) issued a Statement of Reasons (SOR) to Applicant detailing a single security concern under Guideline E (Personal Conduct). The action was taken 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) implemented by the DOD on June 8, 2017.

Applicant responded to the SOR in writing (Answer) on an unknown date, denied the single allegation, and requested a hearing before an administrative judge. Department Counsel was prepared to proceed on July 24, 2025. The case was assigned to me on July 29, 2025. The Defense Office of Hearings and Appeals (DOHA) issued an initial Notice of Hearing on August 20, 2025. A subsequent Notice of Hearing was issued on November 18, 2025. I convened the hearing as scheduled on January 12, 2026. The

Government offered Government Exhibits 1 through 5, which were admitted. Government Exhibit 2 was admitted over an objection. (Transcript (Tr. One) at 9-12.) Applicant testified on his own behalf and submitted Applicant Exhibits A through H. Applicant Exhibits A through D and F through H were admitted. Admission of Applicant Exhibit E was reserved. The case was continued so that Applicant could obtain a transcript of a telephone call that was recorded by him with the consent of the parties, further described below. (Applicant Exhibit I.) DOHA received the transcript of this hearing on January 23, 2026.

A subsequent Notice of Hearing was issued on January 13, 2026. The case reconvened on January 30, 2026. Applicant testified and submitted Applicant Exhibit I, which was admitted without objection. Applicant Exhibit E was also admitted without objection. The transcript of this hearing (Tr. Two) was received on February 17, 2026. The record closed on January 30, 2026. The hearing and decision were delayed when all administrative judges were furloughed from October 1 through November 12, 2025, during a Federal government shutdown due to a lapse in Federal funding.

Procedural Ruling

At the end of the Applicant's case-in-chief, Department Counsel made a motion to amend the SOR pursuant to Directive, paragraph E3.1.17, Additional Procedural Guidance. The amendment added a single allegation under Guideline K, Handling Protected Information, which incorporated the single allegation under Guideline E, Personal Conduct. The amendment was allowed over an objection by Applicant, who denied the allegation. (Tr. Two 155-158.)

Findings of Fact

Applicant is 40 years old, married, and has five children. He has two bachelor's degrees and one master's degree. He has been employed by a defense contractor as a cyber systems engineer since March 2023. He was employed by another defense contractor (Company A) from January 2020 through February 2023. He was employed by Company A when the incidents involved in the SOR took place, (Government Exhibit 1 at Sections 12, 13A, 17, and 18.)

Paragraph 1, Guideline E (Personal Conduct)

The government alleges in this paragraph that Applicant is ineligible for clearance because he engaged in conduct that involves questionable judgment, lack of candor, dishonesty, or unwillingness to comply with rules and regulations.

Paragraph 2, Guideline K (Handling Protected Information)

The government alleges in this paragraph that Applicant is ineligible for clearance because he engaged in conduct that shows a deliberate or negligent failure to comply with rules and regulations for handling protected information. This includes classified and other sensitive government information, and proprietary information.

The single allegation in the SOR states as follows:

a. From about July 2022 until about November 2022, you failed to conduct required computer audits while working as a Security Administrator at [B] Air Force Base. Following an investigation, it was determined that you had demonstrated willful negligence and lack of understanding of assigned roles and responsibilities as a Security Administrator. As a result, your access to [B] Air Force Base was revoked.

During the time in question, Applicant was a member of a three-person security team (Applicant, Mr. C, and Mr. S) that had certain digital security responsibilities at B Air Force Base. These security responsibilities involved conducting audits of various information technology (IT) systems. The audits in question were to be conducted on a daily or weekly basis depending on the system. Beginning in July 2022, it is alleged that the team began conducting audits on various systems on a weekly basis, instead of the required daily basis. In fact, evidence was introduced showing that there were large swaths of time when no audits were being conducted. (Government Exhibit 5 at 3-4; Applicant Exhibit F at 7-11; Applicant Exhibit I at 4-6, 8, 10; Tr. One at 37-39, 41; Tr. Two at 13, 43-45.)

This issue was discovered by Applicant's supervisor (Supervisor), who was physically located in another state. The Supervisor notified Applicant of this issue during a text message exchange on November 15, 2022. (Applicant Exhibit A; Tr. One at 54-63; Tr. Two at 75-77.)

Subsequent to the discovery that the required audits had not been conducted, there was a telephone call between Applicant, his Supervisor, Mr. C, and other employees of Company A. This telephone call was recorded by Applicant, with the permission of other people on the call. A transcript was made of the call and submitted into evidence as Applicant Exhibit I. (Tr. Two at 9-10.)

After this telephone call an investigation was conducted by Company A and the Air Force unit involved, who was the customer. (Government Exhibit 5.) Based on that investigation, the decision was made to terminate the access of Applicant and Mr. C to B Air Force Base. On February 14, 2023, the Air Force unit involved reported the decision regarding Applicant in the Defense Information System for Security (DISS) as follows:

The National . . . Support Center . . . conducted an assessment regarding the auditing protocols taking place in six (6) assigned Squadron Operating Units (SOUs). During the assessment, it was determined that there were significant gaps of time where none of the daily and weekly required audits were conducted. This assessment was supported from audit logs which were pulled directly from . . . The results of the assessment indicate two issues: willful negligence and lack of understanding of assigned roles and responsibilities as an . . . Security Administrator. Both issues present significant risk to the mission of [the Air Force units involved] as a whole. As such, Air Force is no longer willing to host the individual found culpable

(Subject) [Applicant] in [the Air Force units involved] Special Access Program Facilities (SAPFs). While there is inherent risk in operating a weapons system the caliber of . . . , we do not intentionally accept risk where integrity and skill are at the foundation of the decision. (Government Exhibit 4.) (See Government Exhibit 5 at 8-9, 11.)

Based on that decision, Applicant's access to B Air Force Base was revoked. He was administratively terminated from his employment on February 21, 2023. (Government Exhibit 5 at 18.)

Applicant argument centers on three different points: (1) there were technological issues that kept him from doing the job; (2) he was doing what his team lead told him to do; and (3) the audits of concern were not his responsibility.

Turning first to the technological issues. Applicant spent a great deal of time arguing in print and during his testimony that the SOU systems were not properly recording his actions when he was logging in and completing his audits. There appears to be some evidence that there were technology issues. However, the extent to which those issues affected Applicant's ability to do his job is not clear. In addition, as stated, the record shows many times when required audits were not done for months, much less daily. Applicant and his colleagues had no explanation for that. Finally, these technology issues were known by both Company A and the Air Force. With that knowledge they each found Applicant had nonetheless acted negligently and that he did not understand his assigned role as a Security Administrator. (Government Exhibit 5 at 12-17; Applicant Exhibit C; Applicant Exhibit F at 9; Applicant Exhibit I at 40-47; Tr. Two at 41-42, 49-50, 70-71 89-90, 149-153.)

Secondly, Applicant also argued that since the decision to move from daily to weekly audits on the subject SOUs was made by the team lead, he had no reason to question the decision, and therefore he was not responsible for the failure to do the audits in a timely manner. First of all, there is evidence in the record that Mr. S, was acknowledged to be the informal team lead. Applicant has consistently stated that Mr. S and Mr. C informed him of the change from daily to weekly audits after he returned from extended leave in late June 2022. In addition, his Supervisor did admit that this was at least partially a management responsibility concerning training and oversight. (Government Exhibit 5 at 1-2, 5-7; Applicant Exhibit A at 6; Tr. One at 39-40, 47-54, 60-68; Tr. Two at 89, 132-133.)

Applicant argues that the transcript of the telephone call (Applicant Exhibit I) supports his statements. In fact, the evidence of that phone call is mixed. A fair reading of the entire transcript indicates that Applicant and Mr. C were not certain of their responsibilities. They were unable to account for the months of time when there was no record of any audits being completed. The transcript also shows that management was struggling to determine the extent of the problem. There is no doubt that Applicant was unsure of his responsibilities. Whether that was his fault, the fault of management, or a combination of the two is unclear from the available record. (Tr. Two at 122-138, 158-159.)

Finally, Applicant argued that he did the audits he was required to do under the revised schedule. That has been his consistent argument. This is somewhat aligned with his argument as to the team dividing up the work. However, as pointed out by his supervisor and confirmed by Applicant, all three of them knew that the proper audit time for the subject SOUs was daily, not weekly. The fact that they had decided among themselves to divide the work does not obviate Applicant's individual responsibility for the whole job, which involved all the subject machines. (Tr. Two at 59, 82, 99-102, 142-143, 165-169.)

Management was concerned about Applicant's failure to confront his co-workers on what was obviously a change from a required activity. Applicant denied that he had any such responsibility. He testified:

I wasn't then [2022] and I'm not now, in a position of leadership, managerial, supervisory or otherwise.

And so, me going in after completing all my work to go verify the work of my colleagues, my coworkers, is outside of my work scope. (Applicant Exhibit I at 31; Tr. Two at 103, 123, 176.)

Mitigation

Applicant presented evidence showing that he is respected by his friends and coworkers. He is described as having good character and judgment. A Classified Cyber Security Manager for Company A stated that Applicant is "an accountable and respected professional." (Applicant Exhibit D at 4; Applicant Exhibit G; Tr. 107-122.)

Finally, Applicant testified that he has taken steps with his new employer to ensure such an incident does not happen again. For example, he stated, "I work much more closely with management now, and have good rapport with my local management here at my job. I am put in a position at work to be able to train new employees that will work in the . . . classified spaces." (Tr. Two at 191.)

Analysis

Paragraph 1, Guideline E (Personal Conduct)

The security concern under this guideline 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.

The guideline notes several conditions that could raise security concerns under AG ¶ 16. One is applicable in this case:

(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.

I considered the following mitigating condition under AG ¶ 17:

(c) the offense was 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.

Paragraph 2, Guideline K (Handling Protected Information)

The security concern under this guideline 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.

I considered the following disqualifying condition under AG ¶ 34:

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

I have considered the following mitigating conditions under AG ¶ 35:

(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 his security responsibilities; and

(c) the security violations were due to improper or inadequate training or unclear instructions.

Applicant is a Cyber Security Engineer. His responsibilities include auditing information systems to make sure there were no intrusions by hostile actors. In 2022, he was part of a three-person team at B Air Force Base. It appears that the team decided to split up the work in auditing all the systems that were assigned to them, though that is unclear based on the available record. What is clear is that after July 2022, the required daily audits were not done in a timely manner. Whether they were done weekly, as Applicant and Mr. C argue, or not at all as Company A states, is not material. What is material is that it was negligent of Applicant to go along with the decision. Disqualifying conditions AG ¶ 16(c) and AG ¶ 34(g) apply. The burden therefore is Applicant's to show that he has mitigated the security significance of his conduct. He has done so.

It is over three years since the confusion over the timing of the audits was discovered based on Applicant's asking for clarification from his management. There is evidence that Applicant's Supervisor admitted that there was inadequate training and supervision of the team, since it was done remotely.

Applicant has had three years to think about what happened here, and it is obvious he has done so. His testimony shows a person who has internalized the issues brought up by his conduct, or lack thereof. Applicant described how he now works to avoid such issues, and helps others avoid them. All of the cited mitigating conditions under both guidelines apply and Guideline E and Guideline K are found for Applicant.

Whole-Person Concept

Under the whole-person concept, the administrative judge must evaluate an applicant's eligibility for national security eligibility 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 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 pertinent facts and circumstances surrounding this case. Applicant is eligible for national security eligibility because he has mitigated his past personal conduct in the handling of protected information. Paragraphs 1 and 2 are found for Applicant.

Formal Findings

Formal findings for or against Applicant on the allegations set forth in the SOR, as required by ¶ E3.1.25 of Enclosure 3 of the Directive, are:

Paragraph 1, Guideline E: FOR APPLICANT

 Subparagraph 1.a: For Applicant

Paragraph 2, Guideline K: FOR APPLICANT

 Subparagraph 2.a: For Applicant

Conclusion

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

WILFORD H. ROSS
Administrative Judge