DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 24-01547
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Nicholas T. Temple, Esq., Department Counsel
For Applicant: Grant Couch, Esq.

09/18/2025

Decision

BORGSTROM, Eric H., Administrative Judge:

Applicant did not mitigate the handling protected information and personal conduct security concerns. Eligibility for access to classified information is denied.

Statement of the Case

On January 3, 2025, the Defense Counterintelligence and Security Agency (DCSA) issued a Statement of Reasons (SOR) to Applicant detailing security concerns under Guideline K (handling protected information) and Guideline E (personal conduct). The DCSA acted under Executive Order (EO) 10865, *Safeguarding Classified Information within Industry* (February 20, 1960), as amended; Department of Defense (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.

In Applicant's January 29, 2025 response to the SOR (Answer), he admitted SOR ¶¶ 1.b., 1.c., 1.f., 2.a., and 2.b., and he denied SOR ¶¶ 1.a., 1.d., 1.e., 1.g., 1.h., 2.c., and 2.d. He provided a statement explaining each alleged incident, but he did not attach any other documentary evidence. He requested a hearing before a Defense Office of Hearings and Appeals (DOHA) administrative judge. (Answer)

On March 28, 2025, the Government was ready to proceed to a hearing. I was assigned this case on April 2, 2025. On April 7, 2025, a notice was issued scheduling the hearing for May 8, 2025, by video teleconference. The hearing proceeded as scheduled. The Government proffered seven evidentiary exhibits, and I admitted Government Exhibits (GE) 1 through 7, without objection. Applicant testified and submitted six exhibits, which I marked as Applicant Exhibits (AE) A through F. AE A through AE E were admitted into evidence, without objection. AE F consists of six character-reference letters. Five of the letters were admitted into evidence, without objection. Department Counsel objected to admission of a three-page letter from the facility security officer (FSO) at Applicant's former employer, because the letter addressed both Applicant's character, work performance, and the alleged security incidents. I admitted into evidence the excerpts of AE F attesting to Applicant's character and work performance, and I excluded all portions specifically containing the FSO's discussion of the security incidents and her opinions about the employer's security environment and workload. I held the record open until June 9, 2025, to give Applicant the opportunity to provide a revised letter from the FSO and any other additional evidence. I received the transcript (Tr.) on May 19, 2025. Applicant timely submitted three post-hearing exhibits, which I admitted as AE G through I, without objection. The record closed on June 9, 2025. (Tr. 18-29)

Amendment to the SOR

During the hearing, Department Counsel sought to amend the SOR to cross-allege the conduct in SOR ¶ 1.a. under Guideline E as SOR ¶ 2.e. Because the hearing had already commenced, I construed Government's proffer as a motion to amend pursuant to Paragraph 17 of the Additional Procedural Guidance of the Directive. Applicant objected to the amendment. Because Applicant was already on notice of the Government's concerns regarding this conduct, I overruled the objection and granted the motion to amend the SOR. I left the record open until June 9, 2025, to permit Applicant the opportunity to respond with additional argument and evidence. (Tr. 70-72)

Findings of Fact

Applicant is 44 years old. He graduated from high school in 1999, and he earned a bachelor's degree in March 2020. He has been married since January 2010, and he has four children, ages 23, 15, 11, and 9. (GE 1, GE 2; AE B; Tr. 30-31)

From March 2000 to May 2020, Applicant served on active duty in the U.S. Air Force, from which he honorably retired. From April 2020 to June 2023, he was employed full time as an industrial security representative with a DOD contractor (Contractor A). He was terminated from this position for violation of a company policy for falsifying business records. Since August 2023, he has been employed as a background investigator with a different DOD contractor. He was first granted a secret clearance in June 2001, and his access was renewed in November 2011. (GE 1; AE B; Tr. 31-33)

The SOR alleges Guideline K security concerns arising from a series of security infractions, security violations, or other failures to adhere to Contractor A's security requirements. The SOR also alleges Guideline E security concerns based on plagiarism

accusations, workplace misconduct, falsifications during his DOD background security investigation, and one of his security incidents.

SOR ¶¶ 1.a. and 2.e. When Applicant was hired and trained as an industrial security representative (ISR) in 2020, one of the responsibilities of the security team was to perform above-ceiling checks for each of the seven rooms designated as a sensitive compartmented information facility (SCIF). Monthly checks were required under the regulations delineated in the National Industrial Security Program Operating Manual (NISPOM). These monthly checks were confirmed at an annual security audit with the customer (the DOD), and the logs were typically presented or made available. Although the NISPOM did not require that an ISR maintain a security log of the monthly above-ceiling checks, Contractor A's FSO or security manager had long required such a log to record the date, time, and individual who performed each check. A security log was maintained in each of the seven rooms requiring monthly checks. Although the format of the log had changed during Applicant's tenure with Contractor A, the requirements to complete and record the monthly checks in the log remained throughout. Beginning in 2020, Applicant had the responsibility to perform the monthly above-ceiling checks, which required him to carry and use a ladder. (Tr. 40-42, 83-84, 103-108, 110, 137)

In late May 2023, in anticipation of a customer security audit, Applicant reviewed the above-ceiling security logs for the seven SCIFs or classified rooms. He then backdated the missing monthly log information from January 2023 to May 2023 for all seven rooms. Applicant testified that he had completed the monthly checks for all seven rooms, but he had not annotated the security logs as required. He claimed that he had not been trained or instructed that he was required to immediately complete the security log upon completion of the above-ceiling check. He admitted backdating the security logs and that he estimated the dates of his checks. (Tr. 40-43, 93-94, 103-108)

Earlier in May 2023 another ISR had been engaged in a self-inspection of one of the SCIFs in anticipation of the customer security audit and had noticed the missing monthly log information and then the completed logs a week later. This discovery was reported to the security manager, and a security investigation was initiated. (GE 6 at 2)

Contractor A's security investigation was completed on June 15, 2023. The investigation relied upon data from the seven room logs from January 2022 to May 2023. For the 119 purported inspections (seven rooms over 17 months), the above-ceiling logs were then reconciled against badge records for each room, badge records for entry into the building, alarm records for each room, and Applicant's own payroll records. This data confirmed that 51 of 119 inspections were completed, 65 inspections were not completed as claimed on the logs, and 3 monthly inspections were missed altogether. Furthermore, 46 of the logged inspections matched up with dates when Applicant was teleworking or not scheduled to work at all. (GE 6 at 2)

As part of the Contractor A's investigation, Applicant was interviewed, and he provided a statement. When interviewed, Applicant admitted that he "filled out the checklists after the fact." He stated that he had timely completed the inspections but had

failed to fill out the security logs at the time of the inspections. He had backdated the logs in anticipation of a security audit. His June 13, 2023 statement, in pertinent part, reads:

> I completed the above ceiling inspection without properly documenting the completion dates on the spreadsheet attached to the room. Our team here is low manned and I complete numerous tasks at one time heading into a room. The documentation portion of the room inspection for specific issues wasn't [a] priority to me at the time. That is my fault. Knowing there was a government inspection coming up I went back to document the inspections I completed but did not know the correct dates. I guessed the dates and wrote them onto the spreadsheet so we would be compliant for the inspection. This was a bad decision and I should have just left the document how it was and explained it to the evaluators. I am sorry for my actions and the decision made. I let my team down as well as myself. (GE 4)

Based on the discrepancies in the log annotations and badge records, the investigation concluded that Applicant "falsified the data on seven classified open storage room ceiling check logs on 65 occasions," failed to properly complete the required checks, and committed seven additional security violations or infractions since January 2023. The investigation also relied on a report by the FSO, as to the seven security incidents (SOR ¶¶ 1.b.-1.h.), discussed below. (GE 5-6)

The Final Report of Security Violation, issued on June 28, 2023, adopted the findings of the security investigation. Based on these findings, Applicant was found to have violated the employer's ethics and business conduct policies when he falsified the security logs. He was terminated on June 28, 2023. (GE 7; AE I; Tr. 54, 110)

At the hearing, Applicant admitted that he backdated the security logs for January to May 2023. When he checked the logs of the seven classified rooms, he noticed that he had not annotated his above-ceiling checks for four or five months. "I believed to the best of my knowledge and belief that I completed those checks. I did not purposely deliberately [sic] try to write in dates that I did not know or that were false on the document." He acknowledged that the investigation concluded that the above-ceiling checks could not have been completed on the dates logged due to badge records and the dates he was not on site. He claimed that his entries may not have been reflected on badge records due to "tailgating" – following another individual into secure area without badging – but that tailgating was prohibited and not done often. He testified that this was the only occasion when he backdated the security logs. (Answer; Tr. 43-44, 81, 84-91, 93, 109-110)

As part of the employer's investigation into the back-dated security logs, the FSO provided a spreadsheet detailing seven security incidents (SOR ¶¶ 1.b.-1.h.). She characterized two incidents as program violations and five as NISPOM infractions, deviations, or violations. She did not identify any specific NISPOM provisions or whether these incidents were infractions or violations. Furthermore, although each incident was assigned a case number, all of seven security incidents were not opened until June 14,

2023, more than two weeks after the investigation was opened into Applicant's back-dating of security logs. (GE 5-7)

SOR ¶ 1.b. In her spreadsheet, the FSO noted that, in January 2023, Applicant failed to alarm a closed area as required and that she had counseled him. In his Answer, Applicant admitted that he failed to alarm the room, and that the FSO had advised him to ensure the room was alarmed. He did not consider their conversation to constitute a formal verbal counseling. He did not receive any documentation concerning the incident, and he was not required to complete any remedial security training. (Answer; GE 5-7; Tr. 46-47)

SOR ¶ 1.c. In her spreadsheet, the FSO noted that, in February 2023, while escorting a facility employee who was not briefed on a special access program, Applicant left the employee alone in a closed area without the required escort. R later reminded Applicant of the escorting procedures. Applicant testified that he escorted a facilities technician into an anteroom within a closed area to replace a paper-towel dispenser. Applicant then stepped out quickly to obtain a writing utensil. He admitted that he later spoke with R about the incident but did not consider their conversation to constitute a formal verbal counseling. He did not receive any documentation concerning the incident, and he was not required to complete any remedial security training. (Answer; GE 5-7; Tr. 47-49)

SOR ¶ 1.d. In her spreadsheet, the FSO noted that, in April 2023, Applicant failed to secure a safe as required. This security incident was reported by a security officer who monitored the closed area. Applicant denied this security incident because he had no recollection of it occurring. He also denied having been verbally counseled for any security infraction or violation for failing to secure a safe. (Answer; GE 5-7; Tr. 49)

SOR ¶ 1.e. In her spreadsheet, the FSO noted that, in April 2023, Applicant failed to alarm a door to a closed area. She reported that she counseled Applicant concerning this security infraction. Applicant admitted he failed to alarm the door as required and that he spoke with her about the incident, but did not consider their conversation to constitute a formal verbal counseling. He did not receive any documentation concerning the incident, and he was not required to complete any remedial security training. (Answer; GE 5-7; Tr. 51)

SOR ¶ 1.f. R reported that Applicant, in April 2023, failed to properly secure coversheets with codewords in the workspace. Applicant admitted that he put the coversheets in the safe but did not spin the lock before he left the closed area. He claimed that there was another individual still working in the area and he had expected that individual would secure the safe. He recalled speaking with the FSO about the incident, but did not consider their conversation to constitute a formal verbal counseling. He did not receive any documentation concerning the incident, and he was not required to complete any remedial security training. (Answer; GE 5-7; Tr. 51-52)

SOR ¶ 1.g. The FSO reported that Applicant, in April 2023, failed to properly sign the Standard Form 702 (security logs) when opening a safe. According to her report, the safe had five secure drawers each with its own security log, and Applicant accessed two drawers and failed to sign the logs for each drawer as required. Applicant denied this security incident and testified that he always annotated the security logs. He did not recall speaking with R about such an incident and denied having been verbally counseled. (Answer; GE 5-7; Tr. 53-54)

SOR ¶ 1.h. The FSO reported that Applicant, between April and May 2023, failed to properly sign the security logs on at least 13 occasions. Security procedures required that Applicant sign the external security logs when accessing the safe and to also sign the internal logs for the removal and distribution of unclassified storage media. Applicant denied this security incident. He explained that he did not sign the external security log each time he removed and distributed storage media because it was "a waste of paper" as this safe was opened frequently. He did not recall speaking with the FSO about such an incident and denied having been verbally counseled. (Answer; GE 5-7; Tr. 53-54, 117-123)

Applicant repeatedly testified that he had not been formally counseled by the FSO or the security manager about any of the incidents alleged. Given his experience in the military, he expected that formal verbal counseling would include an opportunity for him to respond or offer a rebuttal. He also testified that he expected to receive documentation for even a verbal counseling. It was his understanding that an individual would receive a warning upon the initial security infraction or violation. Upon a second security infraction or violation, the individual's supervisor would be notified, and the individual would be required to complete remedial security training. Several violations may result in access being suspended. A security infraction was a lesser offense than a security violation. He stated he only had casual conversations with the FSO about the security incidents, and he was never required to complete remedial security training. (Tr. 55-56, 73-75, 130-135)

SOR ¶ 2.a. In 2019, while taking online college courses, Applicant received three warnings from two different instructors regarding plagiarism. One warning stemmed from his failure to include a footnote in a bibliography for a passage he quoted in an essay. Two additional warnings occurred concerning a different essay for not properly footnoting quotations. All three incidents were reported in his school record, and he was warned that any further incidents may result in his dismissal. He explained that all three incidents were unintentional and prompted him to learn how to properly cite quotations in his papers. (Answer; GE 2 at 6-7; Tr. 57-58, 124-125)

SOR ¶ 2.b. Applicant testified that he and the FSO had been "overloaded" with work, resulting in a heated discussion in February 2023. He admitted that his raised voice was inappropriate for the workplace, but he denied using any profanity. He discussed the incident with the facility security manager and with human resources. By email dated February 21, 2023, Applicant's supervisor (the security manager) wrote, in pertinent part, to Applicant:

> You have been counseled on your inappropriate behavior in the workplace and you reassured us this was an isolated incident and will not happen in the future. You were informed there may be more severe consequences if this behavior continues. (GE 3)

Applicant admitted his inappropriate behavior and that he was required to sign a memorandum stating that such conduct would not recur. He denied that he was formally counseled or reprimanded. He testified that he was not required to participate in any employee assistance program, and no other punishment occurred. (Answer; GE 3; Tr. 59-60, 111-112, 115-116)

SOR ¶ 2.c. On the spreadsheet of security incidents, the FSO reported that the security manager had raised concerns about Applicant's charging of time. According to the security manager, Applicant was leaving early on days he was not on site, and she verbally reprimanded Applicant in April 2023 about mischarging his time. Applicant denied that he mischarged his time. He worked every other Friday on site, and otherwise he had a flexible schedule. On some occasions, he was permitted to telework. He denied having been verbally reprimanded for mischarging his time. (Answer; GE 5-7; Tr. 61-62)

SOR ¶ 2.d. On February 8, 2024, Applicant was interviewed by an authorized investigator on behalf of the Office of Personnel Management (OPM). He admitted that he had been fired in June 2023 for falsification of records in violation of his employer's ethics policies. He further admitted that he completed the required physical inspections, forgot to annotate the logbook as to the inspections, and later backfilled the logbook for the month of March 2023 in preparation for a security audit. He averred that he did not forget to complete the logbook for any month besides March 2023, even after the OPM investigator confronted him with the investigative findings that many of the required inspections had not been completed. When confronted about investigative findings that he did not complete the logbook or door tags from December 2002 through March 2023, he denied this accusation. (GE 2 at 9-11)

During the OPM interview, Applicant denied any verbal counseling or disciplinary actions prior to his June 2023 termination. The investigator then confronted him about eight incidents when he was counseled or reprimanded by his supervisor.

1. When confronted about receiving a verbal reprimand in April 2023 for leaving early from work [SOR ¶ 2.c.], he denied both the alleged verbal reprimand and the underlying misconduct.

2. When confronted about a May 2023 security violation for a piece of unmarked storage media and for failure to fill out a media security log [SOR ¶ 1.h.], he admitted the incident and claimed that he did not consider his conversation with the facility security officer to constitute a verbal counseling.

3. When confronted about an April 2023 incident, when Applicant forgot to complete the requisite security logs after he opened a classified safe [SOR ¶

1.g.], he admitted the incident and claimed that he did not consider his conversation with the FSO to constitute a verbal counseling.

4. When confronted about an April 2023 incident, when a safe room was left open [SOR ¶ 1.d.], Applicant admitted that he was held culpable as the assistant FSO. He denied he personally left the safe open. He did not consider his conversation with the FSO to constitute a verbal counseling.

5. Applicant was confronted about another April 2023 incident, when a closed room was left open and unalarmed [SOR ¶ 1.e.]. Applicant was found culpable, though he claimed that he directed a security guard to secure the door. He did not consider his conversation with the FSO to constitute a verbal counseling.

6. Applicant was confronted about leaving a facility employee, who had not been briefed into a specific program, alone in a closed area without the required escort in February 2023 [SOR ¶ 1.c.]. During the interview, he stated that he did not recall the incident.

7. Applicant was confronted about leaving a closed room unalarmed in January 2023 [SOR ¶ 1.b.]. He stated that he did not recall this incident.

8. Applicant was confronted about a heated confrontation with another employee in February 2023 [SOR ¶ 2.b.], when he allegedly yelled profanities at the FSO. He admitted that they had gotten into a heated argument and that the FSO had cried. He denied that he had used any profanity. He admitted speaking with the security manager, but stated that he had not considered this a verbal counseling. (GE 2 at 9-11)

In his October 4, 2024 response to DOHA interrogatories, Applicant admitted that the OPM interview summary accurately reflected the information he provided during his February 8, 2024 interview. He made no corrections to any portion of the summary. He added that he did not consider his conversations with the FSO to constitute an official reprimand in reference to the eight incidents above. (GE 2 at 13-14)

At the hearing, Applicant admitted that he had been aware of the security incident regarding the above-ceiling checks and the plagiarism warnings at the time of his OPM interview. He denied that he had been aware of the seven security infractions or violations recorded by the FSO, and he denied that he was verbally counseled for any of these incidents. He admitted that the security manager presented him with a memorandum, which he signed, documenting the workplace inappropriate behavior (SOR ¶ 2.b.). He acknowledged that he had received a verbal counseling for his inappropriate behavior. When questioned about his failure to disclose the verbal counseling during his OPM interview, he testified that he had been "thrown off" by all of the security incidents raised by the OPM investigator. He added that he did not disclose the inappropriate behavior incident during because he "didn't receive the documentation that was signed by me and

my supervisor." He claimed that the inappropriate behavior incident was not memorable because he did not suffer any repercussions. (Tr. 76-80, 111-112)

Applicant testified that he had neither Article 15 actions nor a formal counseling during his military service. He had no security infractions or violations during his military service or with his current employer. He described his work environment with Contractor A as fast paced, as the security team oversaw the security for approximately 300 employees at the facility. He had gotten along well with his previous security managers beginning in 2020, and he had received promotions in July 2022 and early 2023. As of 2022, his titles were senior ISR, alternate facility security officer (AFSO), and classified program security officer. As AFSO, he assisted in logging and identifying security infractions and violations, and he was tasked with logging any violations during the FSO's absence; however, none happened while he was AFSO. Applicant was unaware that the FSO had kept a log of different infractions by Applicant. In January 2023, the security manager began her duties and sought to bring in her own people to serve on the security team. (Tr. 32-33, 38, 45, 67, 98-102)

On his August 5, 2023 security clearance application, Applicant reported his termination for falsification of records. At the hearing, he submitted a current resume that lists his prior employment with Company A ending in August 2023 with no breaks in employment. (AE B, AE E)

Whole Person

Applicant submitted awards and performance evaluations received during his military service and while a civilian employee. He earned two Army Commendation Medals and at least three Air Force Commendation Medals for meritorious service. As a civilian employee, he received several awards for his work performance. He submitted two performance evaluations from his military service. He was found to have exceeded expectations and was recommended for promotion. (AE A, AE C)

In two performance evaluations from his current employer, Applicant's supervisor praised his work performance as "great" and "fantastic" as a background investigator. (AE B, AE G)

Applicant submitted seven character-reference letters from former co-workers and supervisors at Contractor A in support of his clearance eligibility. They praised his work performance, dedication, expertise, honesty, integrity, work ethic, and reliability. They noted his "exceptional dedication to safeguarding classified information and upholding security protocols." The former FSO at Contractor A attested to his reliability and trustworthiness, and she trusted him to safeguard classified information. (AE F, AE H; Tr. 35-37)

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 sensitive 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 sensitive information. Decisions include, by necessity, consideration of the possible risk the applicant may deliberately or inadvertently fail to safeguard sensitive information. Such decisions entail a certain degree of legally permissible extrapolation of potential, rather than actual, risk of compromise of sensitive 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 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 several conditions that could raise security concerns under AG ¶ 34. The following are potentially applicable in this case:

> (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.

In ISCR Case No. 11-05079 at 4 (App. Bd. June 6, 2012), the Appeal Board addressed the need to protect sensitive information even if its protection and handling are not specifically governed by regulations:

> By its plain language, Guideline K acknowledges the need to protect sensitive as well as classified information, notwithstanding the fact that many more rules and regulations have been promulgated to govern the handling of the latter as opposed to the former. Much conduct that is antithetical to the protection of classified or sensitive information may not be contemplated by specific rules or regulations. It need not be. Security significant conduct may be ascertained through the application of common sense with reference to the broad, overall goal of protecting such information. ISCR Case No. 11-05079 at 6 (App. Bd. Jun. 6, 2012)

The SOR alleges Guideline K security concerns arising from a series of eight incidents (SOR ¶¶1.a.-1.h.). The gravity, security significance, and investigation of these incidents varies widely and thus they will be treated distinctly.

For SOR ¶¶ 1.b.-1.h., I found that the security infractions or violations were established by substantial evidence through Applicant's admissions and the FSO's report. A security infraction or violation may occur even if an individual is unaware of the transgression or the occurrence. An infraction or violation is not diminished because enforcement has recently heightened or because an individual's workload is significant. The Government established by substantial evidence that Applicant failed to comply with security requirements and regulations. AG ¶ 34(g) applies as to SOR ¶¶ 1.b.-1.h.

Two weeks after the security investigation was launched on May 30, 2023 into allegations that Applicant had falsified the above-ceiling security logs, the FSO submitted a list of eight additional incidents that occurred between January 2023 and May 2023. The investigations or cases for these incidents were opened on June 14, 2023. There is

no other documentation, including records or emails, regarding these incidents. These circumstances do not undercut the evidence that security infractions or violations occurred; however, the recordkeeping and timing is relevant is determining whether Applicant was counseled or reprimanded as claimed.

AG ¶ 34(h) applies when negligence or lax security practices persist despite counseling by management. When an individual is counseled following an infraction or violation, the counseling serves both to notify the individual of the problem and to inform or educate the individual, so the violation does not recur. In the present case, Applicant was alerted to the infractions through his conversations with the FSO shortly after the incidents occurred. Given his position as an ISR and AFSO, there is no evidence that Applicant did not understand his lapses leading to the infractions or violations. While a more formal verbal counseling or documentation may have served to alert Applicant to the seriousness of his negligence or lax security practices, he was certainly on notice as to his violations and had been adequately trained how to avoid the recurrence of such lapses. Given Applicant's repeated lapses and his acknowledgement of conversations with the FSO about these violations, I conclude that AG ¶ 34(h) applies.

The misconduct alleged in SOR ¶ 1.a. is multilayered. Applicant admitted that he failed to properly log his above-ceiling security checks. He repeatedly stated that he completed the checks but did not timely annotate the logs. At a minimum, Applicant's failure to complete the security logs violated Contractor's A security requirements.

Beyond the admitted back-dating of the security logs, Contractor A's security investigation found that Applicant's conduct constituted a falsification because the above-ceiling security checks were not actually completed. A falsification does not occur by mistake or mis-recordation of a date. Rather, a falsification requires specific intent by Applicant to record an above-ceiling security check on an incorrect date or when not completed at all. Contractor A's security investigation relied upon data from the room entry badge records, building entry badge records, alarm records, and personnel (leave) records when reviewing the above-ceiling logs for January 2022 to May 2023. The investigation found that Applicant had falsified these logs on 65 occasions because he had not performed the requisite above-ceiling checks, relying on the data above. A company's security investigation should be given deference. *See*, *e.g.*, ISCR Case No. 15-08385 at 4 (App. Bd. May 23, 2018)("[B]ecause of the unique position of employer as actual administrators of classified programs and the degree of knowledge possessed by them in any particular case, their determinations and characterizations regarding security violations are entitled to considerable defense and should not be discounted or contradicted without a cogent explanation.").

Here, Contractor A's security investigation did not find a security violation but found violation of a company policy due to the falsification of the security logs. Therefore, the same deference may not be warranted. Nonetheless, the investigation's reliance upon the badge and alarm records is compelling. I also considered that the 65 discrepancies found extends beyond the January to May 2023 period (five monthly checks for seven rooms), which Applicant claimed to have backfilled the security logs. I have also

considered and discounted Applicant's explanation that the numerous discrepancies are attributable to him "tailgating" another employee. He himself noted that "tailgating" was a prohibited practice, particularly in a SCIF.

Most importantly, I have considered Applicant's credibility during the OPM security investigation. During his OPM security interview, he stated that he only back-dated one month of above-ceiling security checks – March 2023. When confronted with Contractor A's investigative findings – that the back-dating covered approximately five months – he continued to contend only one month was affected. He confirmed the accuracy of the interview summary in his response to DOHA interrogatories. I also find that Applicant's representation on his resume – that he worked without interruption at Contractor A and then his current employer – undercuts his credibility. Taken in its entirety, the record evidence established that Applicant failed to comply with Contractor A's security requirements and falsified the above-ceiling security logs on multiple occasions when he did not complete the requisite inspections. AG ¶ 34(g) applies.

Although Department Counsel argued for the application of AG ¶ 34(i), the Government did not establish damage to national security. AG ¶ 34(i) does not apply.

The following handling protected information mitigating conditions under AG ¶ 35 are potentially 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;
>
> (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.

"When the record evidence establishes that an applicant has previously mishandled classified information or violated a rule or regulation for the protection of protected information such an applicant bears a heavy burden in demonstrating that he or she should once again by found eligible for a security clearance." ISCR Case No. 11-12202 at 5 (App. Bd. Jun. 23, 2014) I have considered that there is no evidence of any security violations during Applicant's 20 years of military service or during his most recent two years of civilian employment. I have also considered the fast-paced work environment and the heightened scrutiny of the new security manager. Nevertheless, Applicant committed several security violations within a five-month timespan, even if prior security

managers had not been as strict. More importantly, Applicant's deliberate falsifications on the security logs are not diminished by his heavy workload. Rather, as an ISR and AFSO, Applicant's security lapses and deliberate falsifications are serious security concerns that cast doubt on his trustworthiness, reliability, and judgment. He has not presented any evidence of remedial security training, and he has not established that his security violations resulted from inadequate security training. None of the handling protected information mitigating conditions apply.

Guideline E: Personal Conduct

The 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. . . .

The guideline notes several conditions that could raise security concerns under AG ¶ 16. The following disqualifying conditions are potentially applicable in this case:

> (b) deliberately providing false or misleading information; or concealing or omitting information, concerning relevant facts to an employer, investigator, security official, competent medical or mental health professional involved in making a recommendation relevant to a national security eligibility determination, or other official government representative; and
>
> (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:
>
> (2) any disruptive, violent, or other inappropriate behavior; and
>
> (3) a pattern of dishonesty or rule violations.

Applicant admitted that he received plagiarism warnings on three occasions for two different essays in 2019. He explained that he included quotation marks around the referenced materials but did not properly cite the sources. He acknowledged his errors and stated that his errors were inadvertent. There is no record evidence establishing that he deliberately failed to cite the sources. I find that the alleged conduct, although admitted, does not rise to the level of disqualifying conduct and is not indicative of a larger pattern

of dishonesty. None of the personal conduct disqualifying conditions apply as to SOR ¶ 2.a.

Applicant admitted that he was counseled for inappropriate workplace behavior in February 2023. AG ¶ 16(d)(2) applies as to SOR ¶ 2.b.

Applicant denied that he was verbally reprimanded by the security manager for mischarging his time in April 2023. According to the FSO's log, the security manager believed Applicant was continuing to leave early even after having been reprimanded. Applicant testified that he had a flexible work schedule and could work from home. I note that there is no data about his badge records and that the investigation into mischarging time was open as of the FSO's entries. I have also considered Applicant's heavy workload and his co-worker's statements about his work ethic. The record evidence did not establish that Applicant mischarged his time. AG ¶ 16(d)(3) does not apply as to SOR ¶ 2.c.

During his February 2024 OPM interview, Applicant denied any verbal counseling or disciplinary actions while employed with Contractor A. Even accepting Applicant's testimony that his conversations with the FSO about security lapses were informal, he was formally counseled by the security manager about his inappropriate workplace behavior in February 2023. He claimed that he had forgotten about this incident when he spoke with the investigator in February 2024. Given the absence of other workplace incidents during his military service or at Contractor A, it is not plausible that his formal counseling in February 2023 was not memorable. The email from the security manager to Applicant confirmed that he had been formally counseled and explicitly warned of severe consequences should the misconduct recur. It had occurred a year prior to his OPM interview, and he was discussing his termination and problems at Contractor A just prior to his denial of any verbal counseling. I did not find Applicant's testimony – that he forgot about his February 2023 counseling – to be credible. AG ¶ 16(b) applies as to Applicant's denial of any verbal counselings while employed at Contractor A [SOR ¶ 2.d.].

As discussed within the AG ¶ 34(g) analysis above, Applicant falsified security logs for the above-ceiling checks when he listed checks which he did not actually complete [SOR ¶ 2.e.]. This conduct constitutes a deliberate falsification under AG ¶ 16(d).

The following personal conduct mitigating conditions under AG ¶ 17 are potentially relevant:

> (a) the individual made prompt, good-faith efforts to correct the omission, concealment, or falsification before being confronted with the facts; and
>
> (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.

Applicant admitted that he had backfilled the security logs, but after he was confronted by the security investigators. He continues to deny that he deliberately falsified the security logs by logging above-ceiling checks completed. AG ¶ 17(a) does not apply.

I have considered that there is no other evidence of inappropriate workplace behavior by Applicant either during his military service or in his civilian employment. I have also considered that the FSO, the individual with whom Applicant argued, provided a character-reference letter in support of his character and clearance-eligibility. AG ¶ 17(c) applies as to SOR ¶ 2.c.

Applicant continues to deny that he deliberately provided false information to the OPM investigator and that he deliberately falsified the security logs. I have also considered that, during his OPM interview, he flatly denied back-filling any month besides March 2023. As noted above, his resume does not reflect a break in employment after his June 2023 termination. Doubts remain as to his reliability, trustworthiness, and judgment. AG ¶¶ 17(a) and 17(c) do not apply to SOR ¶¶ 2.d. and 2.e. Applicant did not mitigate the personal conduct security concerns.

Whole-Person Concept

Under the whole-person concept, the administrative judge must evaluate an applicant's eligibility for access to classified information 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 and the factors in AG ¶ 2(d) in this whole-person analysis.

Applicant honorably retired from the U.S. Air Force after 20 years of active-duty service. While thriving for two years as an ISR, he was twice promoted. He presented several character-reference letters attesting to his work performance and character. Between January 2023 and May 2023, he committed several security violations and infractions, was counseled for inappropriate workplace behavior, and falsified security

logs. When questioned about his past employment, he denied any verbal counseling during the OPM investigation. He continues to deny that he deliberately provided false information to the OPM investigator. Doubts remain as to his trustworthiness, reliability, and judgment. He did not mitigate the handling protected information and personal conduct security concerns. Eligibility for access to classified information is denied.

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:	AGAINST APPLICANT
Subparagraphs 1.a.-1.h.:	Against Applicant
Paragraph 2, Guideline E:	AGAINST APPLICANT
Subparagraphs 2.a.-2.c.:	For Applicant
Subparagraphs 2.d.-2.e.:	Against Applicant.

Conclusion

In light of all of the circumstances presented by the record in this case, I conclude that it is not clearly consistent with the interests of national security to grant Applicant's eligibility for a security clearance. Eligibility for access to classified information is denied.

Eric H. Borgstrom
Administrative Judge