DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
REDACTED	)	ISCR Case No. 21-00277
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Carroll J. Connelley, Esq., Department Counsel
For Applicant: *Pro se*

07/19/2022

_____

Decision

_____

MATCHINSKI, Elizabeth M., Administrative Judge:

Applicant exited a secured area while holding classified documents on one occasion in April 2018. His security violation in that regard was inadvertent, but his failure to self-report his security violation continues to cast doubts about his security clearance eligibility. Clearance eligibility is denied.

Statement of the Case

On May 25, 2021, the Defense Counterintelligence and Security Agency Consolidated Adjudications Facility (DCSA CAF) issued a Statement of Reasons (SOR) to Applicant, detailing the security concerns under Guideline E, personal conduct, and Guideline K, handling protected information, and explaining why it was unable to find it clearly consistent with the interests of national security to grant or continue his access to classified information. The DCSA CAF took the action 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 *National Security Adjudicative Guidelines for Determining Eligibility for Access to Classified*

Information or Eligibility to Hold a Sensitive Position (AG) effective within the DOD on June 8, 2017.

On August 17, 2021, Applicant answered the SOR allegations and requested a hearing before an administrative judge from the Defense Office of Hearings and Appeals (DOHA). On March 1, 2022, the Government indicated it was ready to proceed to a hearing. On March 18, 2022, the case was assigned to me to conduct a hearing to determine whether it is clearly consistent with the national interest to grant or continue a security clearance for Applicant. After some coordination of schedules with the parties, on May 12, 2022, I scheduled a hearing for June 7, 2022.

I convened the hearing as scheduled. Three Government exhibits (GE 1-3) and one Applicant exhibit (AE A) were admitted in evidence without any objections. Applicant, his spouse, and his supervisor testified, as reflected in a hearing transcript (Tr.) received on June 23, 2022.

Findings of Fact

The SOR alleges under Guideline E (SOR ¶ 1.a), and cross-alleges under Guideline K (SOR ¶ 2.a), that, in about April 2018, Applicant committed a security violation by exiting a classified area with classified papers in his possession, and that he failed to self-report that violation to his facility security officer (FSO). After considering the pleadings, exhibits, and transcript, I make the following findings of fact.

Applicant is a 61-year-old senior engineer. (GE 1; Tr. 43.) He and his spouse married in September 1994, and they have two sons, ages 30 and 28. Applicant was awarded an associate's degree in October 1991, a bachelor's degree in May 2002, and a master's degree in October 2012. He served in the U.S. Army Reserve from July 1979 to February 1982, when he enlisted in the U.S. Navy. He retired after 20 years of active-duty service in May 2002. He started working for his current employer, a defense contractor, in September 2003. He held a top-secret clearance when he was in the Navy and for his work with his employer until 2018. He was granted access eligibility for sensitive compartmented information (SCI) in December 2016. In April 2018, his clearance eligibility was downgraded to the secret level; his SCI access eligibility was withdrawn; and he was removed from a classified program following his commission of a security violation in April 2018. (GE 1, 3; Tr. 55-56.) The details of the April 2018 incident are as follows.

Because of his experience, high level of clearance, and work demands, Applicant was tasked with working on a classified project as well as carrying out his normal duties in April 2018. (GE 3; AE A.) That project required him to access a closed area outside of his normal worksite. (Tr. 24-25, 41.) Shortly before 11 a.m. on Monday, April 16, 2018, Applicant exited a closed area (SCI facility (SCIF)) with working papers containing information classified at the secret level. He intended to destroy the classified working papers. He was out of the closed area for about eight seconds when he noticed his "mistake," returned to the closed area, and dropped the documents in a bin authorized for destruction of classified documents. Around noontime on April 17, 2018, Applicant asked

two "seasoned" program personnel (co-workers X and Y) about what was required if he had exited a closed area with papers containing information classified at the secret level. Applicant was told by co-worker X to immediately report the action to security officials; that it made no difference if he retained control of the information; and that he could not attempt to circumvent security requirements. About an hour later, co-worker X informed a security official at work about his concern that Applicant possibly deviated from security requirements and did not report the incident. (GE 2.)

On Thursday, April 19, 2018, an all-hands security meeting was held with cleared personnel to reiterate the security policies while working in the closed area and to remind them about the requirement to self-report any deviations or incidents. All attendees at the meeting, including Applicant, were encouraged to be more security conscious and reminded of their responsibilities for handling sensitive and classified information. By the day's end, Applicant had not reported his security violation to his program manager or to security managers. (GE 2.)

Applicant had a scheduled day off from work on Friday, April 19, 2018. When he returned to work on April 23, 2018, he was informed by security personnel about his violation, which he was required to self-report. Applicant provided a written statement to security officials in which he explained that he did not self-report the incident as he "did not know the seriousness of the matter." He indicated that "soon afterwards," he discussed the matter with two peers, who told him to self-report. However, he did not believe it was a security infraction because he had maintained control of the document. He further explained that after reading a warning sign against removing classified material from the secure area (including classified "Yellow Paper"), which was posted on the inside exit door of the closed area, and attending the all-hands security meeting, he determined self-reporting was necessary, but he was off from work on that Friday, April 19, 2018. As to why it happened, Applicant stated:

> This occurred simply because I walked the wrong way. I intended to destroy the working copy that I was using and ended up walking a more familiar route to exit the area. Although I now know the seriousness of this event, and had the chance to self-correct, at the time I treated the classified material as a normal courier. To make things worse, I disregarded peer help to self-correct. I put myself, my reputation and my standing before what was the right thing to do regarding this physical security matter. (GE 2.)

In accord with its reporting requirements under Intelligence Community Policy Guidance (ICPG) 704.2, Applicant's employer issued a security access eligibility report (SAER) to the DOD on May 10, 2018, concerning Applicant's security violation and failure to self-report. The security manager who authored the SAER expressed concerns about Applicant's judgment and integrity. When asked whether he had exited the closed area with a classified "Yellow Paper," Applicant was very reluctant to admit his conduct and tried to rationalize why he did it. The security manager found it troubling that Applicant did not realize the seriousness of the incident. Applicant reportedly questioned the security official about where it stated that "Yellow Paper" could not be removed from the closed area even

though initial and refresher security briefings stressed that such material could not be removed, and that the use of "Yellow Paper" was spelled out in the closed area's standard operating procedures, which Applicant read and acknowledged on being briefed into the program. The security manager also reported that Applicant exhibited a lack of candor with co-worker X by denying, when asked, whether he had removed classified material from the closed area. Co-worker X recounted in a written statement, which was appended to the SAER, that after he told Applicant to immediately turn around, return to the secure space, and report his action to security, Applicant countered with an apparent inquiry about "even if he retained control of the information." Co-worker X did not indicate in his written statement that Applicant expressly denied having exited the secure space with a paper containing secret information. (GE 2.) Applicant maintains that he never denied exiting the closed area with the classified paper or said "anything like that." (Tr. 53.)

Video-surveillance of the door to the closed area showed that only eight seconds passed between Applicant's exit from, and return to, the closed area with the classified papers in hand, but the security manager concluded that the risk of compromise of classified information could not be completely discounted, as visual surveillance could not be validated for about three seconds of time. Applicant's employer issued a written reprimand to Applicant; placed him in a probationary status for six months; and removed him from the program. (GE 2.)

On July 6, 2020, Applicant completed a Questionnaire for National Security Positions (SF 86) for reinvestigation of his clearance eligibility in light of his April 2018 security violation and failure to self-report. He responded negatively to an SF 86 inquiry into whether his security clearance eligibility or access authorization had ever been denied, suspended, or revoked, but commented as follows:

> Following a 2018 violation, I was administratively downgraded from TS to S, and removed from a program. I have since left that department at the company. (GE 1.)

During a July 29, 2020 interview with an authorized investigator for the Office of Personnel Management (OPM), Applicant stated about the April 2018 incident that he walked out of a SCIF with his lunchbox and folder without realizing that the folder had a yellow cover sheet. His intention was to find a microwave for a working lunch. Seconds later, he returned to the SCIF when he realized his mistake. He attributed his failure to self-report the violation to wanting to know what kind of violation he had made before reporting it, and explained that he could not verify that it was an infraction as there was no written procedure in place that such materials could not leave the SCIF. He asserted that when asked by a security manager at work whether he had exited the closed area with classified information, he explained that he could not find a local instruction of an infraction in that regard. During his OPM interview, Applicant expressed regret for his April 2018 actions and admitted that he had plenty of chances to report the incident. He denied any risk of recurrence as he "learned a valuable lesson." (GE 3.)

At his hearing, Applicant explained about the April 2018 incident that he had put his lunchbox on his shoulder and was walking to the microwave for a working lunch and that he never intended to leave the closed area with classified material. (Tr. 40.) He was under schedule stress due to stalled and overdue projects on which he worked part time. He found it "impossible [to] work both projects at the same time and would timeshare days between them." He acknowledged that the proper procedure would have been to ask someone in the closed area to handle his classified material for him when he left the area, but he "did not know many employees there" and so did not ask anyone to hold classified material for him. Normally, he locked up his work when away from his temporary desk in the closed area. (AE A; Tr. 41-42.) He testified that after the incident, he could find "nothing in any procedure, written or otherwise, that classified material couldn't leave the SCIF." (Tr. 46.)

Applicant still feels shame and regret over the April 2018 incident. (Tr. 40.) He expressed his understanding that neither his guilt over the incident nor workplace stress justifies his failure to self-report. He explained that he acted on his "personal self and knowledge of right and wrong pertaining to the many security procedures in place" gained from his security responsibilities and duties through the years, and he could find nothing in his procedures, written or otherwise, that prohibited classified material from leaving the SCIF. (AE A; Tr. 42, 46.) Yet, he admitted on cross-examination that, based on many years of having a clearance and security training, he did not believe he was allowed to take classified information from the SCIF; that he knew it was a security violation; and that he knew he had to report it. (Tr. 47.) As to why the all-hands security briefing of April 19, 2018, did not prompt him to report the incident, Applicant responded,

> I—I think that—you know, that the amount of seconds had something to do with it. I think that, you know, it's a lack of judgment on my part. It was—it was the---you know, the schedule and the problems I was having in a number of areas. I think that there was just a load on my mind, and---and it was just downright bad judgment and wrong. (Tr. 50.)

Applicant disputes the security manager's characterization that he was reluctant in admitting that he exited the closed area with classified papers in hand on April 16, 2018. He asserts that looking for a security instruction or procedure was something he had been doing for about 40 years; that he knew he did wrong but that he was trying to find out how bad his violation was, and he "ran out of time" in that security got to him first. (Tr. 52-53.)

Applicant moved into his current work group in 2020. He held a secret clearance with no issues until the SOR was issued. (Tr. 38.) His supervisor attests that Applicant has been a very reliable worker who takes pride in his work. He requests additional work if he is finished with his assigned tasks, which currently do not require him to hold a security clearance. (Tr. 32-33.) If Applicant's clearance eligibility is adjudicated favorably, it would allow him to work on classified projects in their group. (Tr. 34.) The supervisor is unaware of the April 2018 security incident. Applicant offered to inform him of the reason for the hearing, but the supervisor thought it best not to know. (Tr. 36.)

Applicant's spouse testified about the seriousness with which Applicant takes his work. To her knowledge, he has never revealed any classified information to her. (Tr. 19-20.) He was "devastated" by the April 2018 incident. She has known him to be a loving and caring person, as evidenced by the fact that they have been staying at her mother's to care for her. (Tr. 20, 24.)

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 in conjunction 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(a), the entire process is a conscientious scrutiny of a number of variables known as the "whole-person concept." The administrative judge must consider all available, reliable information about the person, past and present, favorable and unfavorable, in making a decision.

The protection of the national security is the paramount consideration. AG ¶ 2(b) requires that "[a]ny doubt concerning personnel being considered for national security eligibility will be resolved in favor of the national security." In reaching this decision, I have drawn only those conclusions that are reasonable, logical, and based on the evidence contained in the record. 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 EO 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).

Analysis

Guideline E: Personal Conduct

The security concerns about personal conduct are set forth in AG ¶ 15, which provides:

> 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.

Personal conduct security concerns under AG ¶ 15 are established in two aspects: (1) Applicant's removal of papers containing information classified secret from a closed area in April 2018; and (2) his failure to self-report the security violation, despite being directed by two experienced co-workers to go immediately to security and report the incident and being reminded of his security responsibilities during an all-hands security briefing held a few days after the incident.

Applicant's failure to self-report and his security violation of exiting a closed area with classified information in his possession, when considered together, support a whole-person assessment of questionable judgment, as contemplated within AG ¶ 16(c), which provides:

> (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.

Mitigating conditions AG ¶¶ 17(c) and 17(d) have some applicability in this case. They provide:

> (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.

AG ¶ 17(c) supplies some mitigation for Applicant's security violation in that it appears to have been an isolated incident in a record of decades of classified access eligibility for Applicant. The circumstances under which the violation occurred were unique only in that it was on a program and a closed area outside of Applicant's usual job duties and work environment. His lack of familiarity with the workers in the SCIF does not mitigate his security violation in that Applicant knew that he should have ensured that the classified material was properly safeguarded before he exited the closed area. If he did not feel that he could ask someone to hold the classified papers for him, then he had an obligation to secure them in a classified storage container or other approved manner before he left the area. AG ¶ 17(d) also has some applicability in that Applicant acknowledges that he removed the classified papers from the closed area. While the risk of compromise of the classified information could not be completely ruled out, video surveillance shows that he was outside of the closed area with the classified information for only eight seconds. He returned to the closed area once he realized his mistake in removing the classified material. The personal conduct security concerns exhibited by his lapse of judgment in removing the classified material are mitigated.

AG ¶ 17(c) cannot reasonably apply in mitigation of Applicant's failure to self-report. He had held a security clearance for decades and SCI access eligibility since December 2016. He would have had many security briefings over the years regarding his responsibilities to report any known or suspected violations. Even assuming that he believed on April 16, 2018, that he may not have committed a violation because he had the documents in his possession during the eight seconds that he was out of the closed area, he would have had good reason to question that belief after his conversation with co-workers X and Y. Co-worker X clearly informed him that he had to report the incident to security personnel. He did not go to security that day or the following day. He did not report it to security personnel even after an all-hands security briefing in which he was reminded of the security requirement to self-report. His failure to self-report was a continuing course of conduct in that it went on until he was confronted by security personnel on April 23, 2018.

Applicant recognizes that neither his guilt nor his stress about the removal of the classified information from the closed area explains his lack of judgment in failing to self-report the violation. However, he displayed, as recently as during his direct testimony at his hearing, an unacceptable tendency to minimize, if not justify, his failure to self-report by claiming that, "as a procedure guy," he wanted to determine for himself what type of infraction he committed, or even whether he had committed a security violation, before going to security; that he could find nothing written which prohibited the removal of classified material from the SCIF; and that he just "ran out of time." By waiting until cross examination to admit that he did not believe he was allowed to remove classified material from the SCIF; knew it was a security violation; and that he had an obligation to report the incident, he undermined his case in reform. Applicant lacks a track record of persuasive evidence showing that he can be counted on to candidly report when it may be personally disadvantageous to him to do so. AG ¶ 17(d) does not fully apply. The personal conduct security concerns raised by his failure to self-report the security violation are not mitigated.

Guideline K: Handling Protected Information

The security concerns for handling protected information are articulated 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 evidence establishes that Applicant committed a security violation when, in April 2018, he exited a closed area with papers containing information classified at the secret level, and by his failure to report that security violation to his employer's security personnel. In addition to the standard operating procedures for the SCIF, which Applicant violated per the SAER, ¶ 5-100 of the *National Industrial Security Program Operating Manual* (NISPOM), DOD 5220.22-M, dated February 2006, as amended, indicates that cleared individuals are responsible for safeguarding information entrusted to them. Under ¶ 5-306 of the NISPOM, access to closed areas is limited to authorized persons who have an appropriate clearance and a need-to-know for the classified information in the area. Persons without the appropriate security clearance and need-to-know must be escorted at all times. Access is controlled to protect and maintain the security of the classified information in the closed area. The objective of perimeter controls is to discourage the introduction or removal of classified material without proper authority. *See* NISPOM ¶ 5-103.

Regarding the failure to self-report, contractors are required under ¶ 1-302 of the NISPOM to report adverse information that comes to their attention concerning cleared employees. NISPOM ¶ 1-303 requires the report of any loss, compromise, or suspected compromise of classified information. To ensure its compliance with those security requirements, Applicant's employer briefed its cleared employees about their obligation to report known adverse information, including about violations of the NISPOM's security requirements. NISPOM ¶ 3-106 specifically requires that prior to being granted access to classified information, an employee is to receive an initial security briefing that includes (a), a threat awareness briefing; (b) a defensive security briefing, (c) an overview of the security classification system, (d) **employee reporting obligations and requirements,** and (e), security procedures and duties applicable to the employee's jobs. The SAER indicates that Applicant had been briefed about his reporting requirements before and after the April 2018 incident. Disqualifying condition AG ¶ 34(g), "any failure to comply with rules for the protection of classified or sensitive information," is established.

Applicant has the burden of mitigating the security concerns raised by his violation of the rules and regulations for handling protected information and his failure to comply with his reporting requirement. AG ¶ 35 provides for mitigation, as follows:

(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.

Applicant's removal of the classified papers from the SCIF was inadvertent in that he did not intend to circumvent security regulations. He realized his mistake almost immediately as he returned to the closed area after only eight seconds. While AG ¶ 35(a) has some applicability in that the violation "happened so infrequently," the importance of reporting a known security violation is clear in AG ¶ 35(d), which requires that even inadvertent security violations be promptly reported. Applicant had several opportunities to report the incident to security officials, and he failed to do so. His efforts to justify or minimize his violation by claiming to security officials on April 23, 2018, that he could find no written procedure or policy, when, in fact, a warning was posted on the door of the closed area, shows that the all-hands security training held on April 19, 2018, had little remedial affect. It was not demonstrated that his security violations were due to improper or inadequate training or unclear instructions. Applicant has yet to demonstrate a positive attitude toward the discharge of his security responsibilities, given his reluctance to admit that he knew he had an obligation to report the violation. The handling protected information security concerns are not fully mitigated.

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 his conduct and all relevant circumstances in light of the nine adjudicative process factors in 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.

Some of the adjudicative process factors were addressed under Guidelines E and K, but some warrant additional comment. Applicant handled classified information for decades before his security violations at issue in this case. His long record of apparent compliance with security regulations weighs in his favor in that he has shown that he can handle classified information appropriately. At the same time, because of his years of experience in handling classified information, he can reasonably be expected to have known to report any derivation, intentional or not, from security requirements. In choosing to ignore the advice of co-worker X to immediately report his removal of classified papers from a closed area, Applicant put his self-interest ahead of his security obligations.

The security clearance adjudication involves an evaluation of an applicant's judgment, reliability, and trustworthiness in light of the security guidelines in the Directive. *See* ISCR Case No. 09-02160 (App. Bd. Jun. 21, 2010). It is not designed to punish applicants for past mistakes or shortcomings. That said, failure to report a deviation or violation of security procedures raises considerable doubts about a person's judgment, reliability, and trustworthiness with regard to protecting classified information. It is well settled that once a concern arises regarding an applicant's security clearance eligibility, there is a strong presumption against the grant or renewal of a security clearance. *See Dorfmont v. Brown*, 913 F. 2d 1399, 1401 (9th Cir. 1990). For the reasons previously discussed, doubts persist as to whether it is clearly consistent with the national interest to grant Applicant eligibility for a security clearance.

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 E:	AGAINST APPLICANT
Subparagraph 1.a:	Against Applicant
Paragraph 2, Guideline K:	AGAINST APPLICANT
Subparagraph 2.a:	Against Applicant

Conclusion

In light of all of the circumstances presented by the record in this case, it is not clearly consistent with the interest of national security to grant or continue security clearance eligibility for Applicant. Eligibility for access to classified information is denied.

_____
Elizabeth M. Matchinski
Administrative Judge