DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 24-01079
	)	
Applicant for Security Clearance	)	

Appearances

For Government: William H. Miller, Esquire, Department Counsel
For Applicant: *Pro se*

01/28/2025

_____

Decision

_____

GALES, Robert Robinson, Administrative Judge:

Applicant mitigated the security concerns regarding handling protected information and personal conduct. Eligibility for a security clearance is granted.

Statement of the Case

On October 30, 2017, Applicant applied for a security clearance and submitted a Questionnaire for National Security Positions (SF 86). On July 18, 2024, the Defense Counterintelligence and Security Agency (DCSA) Consolidated Adjudication Services (CAS), renamed the DCSA Adjudication Vetting Services (AVS), issued a Statement of Reasons (SOR) to him under Executive Order (Exec. Or.) 10865, *Safeguarding Classified Information within Industry* (February 20, 1960), as amended and modified; DoD Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (January 2, 1992), as amended and modified (Directive); and Directive 4 of the Security Executive Agent (SEAD 4), *National Security Adjudicative Guidelines* (December 10, 2016) (AG), effective June 8, 2017.

The SOR alleged security concerns under Guideline K (Handling Protected Information) and Guideline E (Personal Conduct), and detailed reasons why the DCSA

adjudicators were unable to find that it is clearly consistent with the national interest to grant or continue a security clearance for Applicant. The SOR recommended referral to an administrative judge to determine whether a clearance should be granted, continued, denied, or revoked.

On July 29, 2024, Applicant responded to the SOR and elected to have his case decided on the written record in lieu of a hearing. A complete copy of the Government's file of relevant material (FORM), including proposed Government Exhibits, identified as Items, was mailed to him by the Defense Office of Hearings and Appeals (DOHA) on September 5, 2024, and he was afforded an opportunity, within a period of 30 days, to file objections and submit material in refutation, extenuation, or mitigation. In addition to the FORM, he was furnished a copy of the Directive as well as the Adjudicative Guidelines applicable to his case. Applicant received the FORM on September 25, 2024. His response was due on October 25, 2024. Applicant chose not to respond to the FORM, for as of November 8, 2024, no response had been received. The case was assigned to me on December 6, 2024, and there was still no response to the FORM.

Findings of Fact

In his Answer to the SOR, Applicant admitted, with comments, the factual allegations pertaining to handling protected information (SOR ¶¶ 1.a. through 1.c.). He failed to address the factual allegations pertaining to personal conduct (SOR ¶ 2.a.) so his failure to comment on those allegations has been treated as though he denied them. Applicant's admissions and comments are incorporated herein. After a complete and thorough review of the evidence in the record, and upon due consideration of same, I make the following findings of fact:

Background

Applicant is a 64-year-old employee of a defense contractor. He has been serving as a principal process engineer since February 1979. He received a bachelor's degree in 1988 and a master's degree in 1998. He has never served with the U.S. military. He has held a secret clearance since at least 2001. He was married in 1991. He has two adult children, born in 1993 and 1996.

Handling Protected Information and Personal Conduct

On March 15, 2018, Applicant signed a Classified Information Nondisclosure Agreement under which he accepted the legal responsibilities and obligations (including proper procedures to be followed) associated with being granted access to classified information. One of those responsibilities covered negligent handling of classified information. (Item 7)

SOR ¶ 1.c. refers to an incident that occurred on July 13, 2020, when Applicant failed to properly secure classified materials when he removed classified hard drives from test equipment that was scheduled to go out to calibration and placed the drives in an unlocked cabinet in the closed area, not approved for open storage. He had difficulty

opening the security container in the area after trying several times and he purportedly did not seek immediate security assistance to properly store the drives. He noted that the secure safe had an older mechanical combination mechanism and that unlocking and opening the older safe had been very problematic prior to the alleged incident. A newer safe/container had been requested several times but no replacement was apparently provided. Applicant claimed that the cabinet he chose to store the hard drives was just as secure as they would have been had they remained in the test equipment rack because everything was still in a closed area.

Applicant disputed the incident report wherein it stated that he did not self-report or attempt to seek immediate security assistance, and he claimed that upon closing the lab, he sent an email to program and security indicating his situation. It was suggested that he bring the hard drives to another safe with a security guard at the entry to the building, but the security guard could not open his safe/container of the same type. Applicant concluded that the hard drives remaining in the storage cabinet within the secured closed area was adequate protection for the evening and the issue could be resolved in the morning with security personnel. (Item 2 at 3; Item 6 at 4) Applicant did not submit any documentary evidence such as a copy of his emails to program and security or any previous requests for a working safe/container.

As a result of the incident, Applicant received a security violation for failing to properly secure classified information in an approved container. This was his first security violation with his employer. He was re-briefed regarding safeguarding procedures and reminded of his continued responsibility to protect classified information. (Item 6 at 4) There is no allegation or evidence that Applicant's actions led to the loss, compromise, or suspected compromise to classified information.

SOR ¶ 1.b. refers to an incident that occurred two months later, on September 17, 2020, when Applicant alarmed the closed area but failed to properly secure the area by not engaging the lock on the door as required. He signed the closed area check record indicating the room was alarmed and the lock was engaged. The unlocked door was discovered by a security officer and a review of the card swipes and the closed area check record revealed that Applicant was the last individual to occupy the closed area. Applicant said he felt positive that he properly secured the closed area and struggled with accepting the mistake. He estimated having opened and closed the secure lab 2,008 times during the four years of working on the program, and the single incident is about 0.05% of those times. He claimed his closing routine is generally very rigorous by checking for re-entry twice after spinning lock, and he had a hard time believing that it was left un-spun, but that he may have been distracted during the process of closing by conversations with colleagues. (Item 2 at 2; Item 4; Item 6 at 3)

As a result of the incident, Applicant received a second security violation and he was required to take closed area training again and for one month he was required to have a "lock up buddy." The employer reported that the incident did not involve the loss, compromise, or suspected compromise to classified information. (Item 4)

SOR ¶ 1.a. refers to four separate incidents that occurred on July 20, 2022; July 26, 2022; August 3, 2022; and November 23, 2022, when Applicant conducted Assured File Transfers (AFTs) but failed to log his actions in the media log as required, violating at least two employer policies. Applicant claims he performed 154 AFTs during the program and security forms were submitted for each AFT, signed by two levels of management and security officer prior to executing an AFT. He suspected that he may have forgotten to make the entries due to interruptions of his routine by colleagues requesting information from him or simply needing to attend to other duties such as testing hardware in the closed area before getting to the log. As a result of his violations, he received a written warning on December 19, 2022, and was retrained on his responsibilities to properly log AFTs. (Item 2 at 2; Item 5; Item 6 at 2) There is no allegation or evidence that Applicant's actions led to the loss, compromise, or suspected compromise to classified information.

Policies

The U.S. Supreme Court has recognized the substantial discretion of the Executive Branch in regulating access to information pertaining to national security emphasizing, "no one has a 'right' to a security clearance." (*Department of the Navy v. Egan*, 484 U.S. 518, 528 (1988)) As Commander in Chief, the President has the authority to control access to information bearing on national security and to determine whether an individual is sufficiently trustworthy to have access to such information. The President has authorized the Secretary of Defense or his designee to grant an applicant eligibility for access to classified information "only upon a finding that it is clearly consistent with the national interest to do so." (Exec. Or. 10865, *Safeguarding Classified Information within Industry* § 2 (Feb. 20, 1960), as amended and modified.)

When evaluating an applicant's suitability for a security clearance, the administrative judge must consider the guidelines in SEAD 4. In addition to brief introductory explanations for each guideline, the guidelines list potentially disqualifying conditions and mitigating conditions, which are used in evaluating an applicant's eligibility for access to classified information.

An administrative judge need not view the guidelines as inflexible, ironclad rules of law. Instead, acknowledging the complexities of human behavior, these guidelines are applied in conjunction with the factors listed in the adjudicative process. The administrative judge's overarching adjudicative goal is a fair, impartial, and commonsense decision. The entire process is a conscientious scrutiny of several 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 meaningful decision.

In the decision-making process, facts must be established by "substantial evidence." "Substantial evidence [is] such relevant evidence as a reasonable mind might accept as adequate to support a conclusion in light of all contrary evidence in the record." (ISCR Case No. 04-11463 at 2 (App. Bd. Aug. 4, 2006) (citing Directive ¶ E3.1.32.1)).

"Substantial evidence" is "more than a scintilla but less than a preponderance." (*See v. Washington Metro. Area Transit Auth.*, 36 F.3d 375, 380 (4th Cir. 1994))

The Government initially has the burden of producing evidence to establish a potentially disqualifying condition under the Directive and has the burden of establishing controverted facts alleged in the SOR. Once the Government has produced substantial evidence of a disqualifying condition, under Directive ¶ E3.1.15, the applicant has the burden of persuasion to present evidence in refutation, explanation, extenuation, or mitigation, sufficient to overcome the doubts raised by the Government's case. The burden of disproving a mitigating condition never shifts to the Government. (*See* ISCR Case No. 02-31154 at 5 (App. Bd. Sep. 22, 2005))

A person who seeks access to classified information enters a fiduciary relationship with the Government predicated upon trust and confidence. This relationship transcends normal duty hours and endures throughout off-duty hours as well. It is because of this special relationship that the Government must be able to repose a high degree of trust and confidence in those individuals to whom it grants access to classified information. Decisions include, by necessity, consideration of the possible risk the applicant may deliberately or inadvertently fail to safeguard classified information. Such decisions entail a certain degree of legally permissible extrapolation as to potential, rather than actual, risk of compromise of classified information. Furthermore, "security clearance determinations should err, if they must, on the side of denials." (*Egan*, 484 U.S. at 531)

Clearance decisions must be "in terms of the national interest and shall in no sense be a determination as to the loyalty of the applicant concerned." (*See* Exec. Or. 10865 § 7) Thus, nothing in this decision should be construed to suggest that I have based this decision, in whole or in part, on any express or implied determination as to Applicant's allegiance, loyalty, or patriotism. It is merely an indication the Applicant has or has not met the strict guidelines the President, Secretary of Defense, and Director of National Intelligence have established for issuing a clearance. In reaching this decision, I have drawn only those conclusions that are reasonable, logical, and based on the evidence contained in the record. Likewise, I have avoided drawing inferences grounded on mere speculation or conjecture.

Analysis

Guideline K, Handling Protected Information

The security concern relating to the guideline for Handling Protected Information is set out in AG ¶ 33:

> *The Concern.* 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 also includes some conditions that could raise security concerns under AG ¶ 34:

> (b) collecting or storing protected information in any unauthorized location;
>
> (g) any failure to comply with rules for the protection of classified or sensitive information;
>
> (h) negligence or lax security practices that persist despite counseling by management; and
>
> (i) failure to comply with rules or regulations that results in damage to the national security, regardless of whether it was deliberate or negligent.

AG ¶¶ 34(b) and 34(g) have been established. Applicant's negligent and inadvertent actions resulted in six security violations during a two-year period. There is no evidence that any of the incidents involved the loss, compromise, or suspected compromise to classified information, thus negating the application of AG ¶ 34(i). Two of those violations – the July 2020 failure to properly secure classified materials in a locked cabinet in a closed area, and the September 2020 failure to properly secure a closed area by engaging the lock on the door – were isolated types of violations that, after receiving written warnings and completing retraining from his employer, were never repeated. The other four violations, on July 20, 2022; July 26, 2022; August 3, 2022; and November 23, 2022 – were, after the first violation, repeated failures to log in his AFTs. It appears that the employer did not issue Applicant written warnings or require retraining after the first such violation, but apparently waited until December 19, 2022, well after the November 2022 violation to do so. Because Applicant's negligence or lax security practices, in general, continued after he received his initial warning and retraining, and he should have become more attentive to his responsibilities, while the violations were not of the identical type, they did persist even after he went through retraining, establishing AG ¶ 34(h).

The guideline also includes some conditions that could mitigate security concerns 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 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.

On July 13, 2020, Applicant failed to properly secure classified materials when he placed hard drives in an unlocked cabinet in a closed area, not approved for open storage. Because he experienced difficulty in opening the security container in the area after trying several times, and was unable to access another appropriate one, he decided to use an inappropriate cabinet because it was protected in the closed area. The isolated situation occurred under unusual circumstances regarding his repeated requests of his employer to furnish a newer safe/container to replace the one that was frequently difficult to use. The inappropriate container was located inside the closed area, but its use was still considered a security violation. The record is silent as to whether there were clear instructions or adequate training to employees in the event such a situation should arise. Applicant responded favorably to remedial security training and a similar security violation has not reoccurred.

With regard to his September 2020 failure to properly secure the closed area, as required, Applicant estimated having opened and closed the secure lab 2,008 times during the four years of working on the program, and the single alleged incident is about 0.05% of those times. He claimed his closing routine is generally very rigorous by checking for re-entry twice after spinning the lock, but that on this one occasion, he may have been distracted during the process of closing by conversations with colleagues. In any event, Applicant responded favorably to remedial security training and a similar security violation has not reoccurred.

There were four separate incidents that occurred on July 20, 2022; July 26, 2022; August 3, 2022; and November 23, 2022, when Applicant conducted AFTs but failed to log his actions in the media log as required, violating at least two employer policies. Applicant claimed he performed 154 AFTs during the program and security forms were submitted for each AFT, signed by two levels of management and security officer prior to executing an AFT. The violations were inadvertent, and he suspected that he may have forgotten to make the entries due to interruptions of his routine by colleagues requesting information from him or simply needing to attend to other duties such as testing hardware in the closed area before getting to the log. Although the violations were repeated, with the first two taking place in July 2022, his employer apparently took no corrective action until December 2022 – approximately five months after the first such violation – to issue a written warning and start retraining. Applicant responded favorably to remedial security training and a similar security violation has not reoccurred.

With respect to all of Applicant's security violations, there is no allegation or evidence that Applicant's actions led to the loss, compromise, or suspected compromise to classified information. Additionally, while there were multiple diverse security violations, all of them were inadvertent and considering the length of time Applicant has had his

responsibilities, his actions do not suggest a pattern of inappropriate procedures. Accordingly, AG ¶¶ 35(a), 35(b), 35(c), and 35(d) have been established.

Guideline E, Personal Conduct

The security concern relating to the guideline for Personal Conduct 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 following will normally result in an unfavorable national security eligibility determination, security clearance action, or cancellation of further processing for national security eligibility:
>
> (a) refusal, or failure without reasonable cause, to undergo or cooperate with security processing, including but not limited to meeting with a security investigator for subject interview, completing security forms or releases, cooperation with medical or psychological evaluation, or polygraph examination, if authorized and required; and
>
> (b) refusal to provide full, frank, and truthful answers to lawful questions of investigators, security officials, or other official representatives in connection with a personnel security or trustworthiness determination.

The guideline also includes conditions that could raise security concerns under AG ¶ 16:

> (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; and
>
> (d) credible adverse information in that is not explicitly covered under any other guideline and may not be sufficient by itself for an adverse determination, but which, when combined with all available information, supports a whole-person assessment of questionable judgment, untrustworthiness, unreliability, lack of candor, unwillingness to comply with rules and regulations, or other characteristics indicating that the individual may not properly safeguard classified or sensitive information. This includes, but is not limited to, consideration of:

> (1) untrustworthy or unreliable behavior to include breach of client confidentiality, release of proprietary information, unauthorized release of sensitive corporate or government protected information;
>
> (2) any disruptive, violent, or other inappropriate behavior;
>
> (3) a pattern of dishonesty or rule violations; and
>
> (4) evidence of significant misuse of Government or other employer's time or resources.

All of the security concerns alleged under Guideline E in the SOR are covered under Guideline K. AG ¶¶ 16(c) and 16(d) do not apply.

Whole-Person Concept

Under the whole-person concept, the administrative judge must evaluate an applicant's eligibility for a security clearance by considering the totality of the applicant's conduct and all the circumstances. The administrative judge should consider the nine adjudicative process factors listed at SEAD 4, App. A, ¶ 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 SEAD 4, App. A, ¶ 2(c), the ultimate determination of whether to grant a security clearance must be an overall commonsense judgment based upon careful consideration of the guidelines and the whole-person concept. Moreover, I have evaluated the various aspects of this case considering the totality of the record evidence and have not merely performed a piecemeal analysis. (*See U.S. v. Bottone*, 365 F.2d 389, 392 (2d Cir. 1966); *See also* ISCR Case No. 03-22861 at 2-3 (App. Bd. Jun. 2, 2006))

I have incorporated my comments under Guideline K and Guideline E in my whole-person analysis, and I have considered the factors in SEAD 4, App. A, ¶¶ 2(c) and 2(d). Applicant is a 64-year-old employee of a defense contractor. He has been serving as a principal process engineer since February 1979. He received a bachelor's degree in 1988 and a master's degree in 1998. He has held a secret clearance since at least 2001. In the national security environment, I am aware that just one security violation can be devastating. While it is clear that Applicant negligently and inadvertently committed multiple diverse security violations between July 2020 and November 2022, there is no allegation or evidence that Applicant's actions led to the loss, compromise, or suspected

compromise to classified information. Moreover, considering the length of time Applicant has had his security-related responsibilities, these relatively isolated actions in 2020 and 2022 do not suggest a pattern of inappropriate procedures. As noted above, after he was retrained by his employer, Applicant responded favorably and did not make the same mistakes.

Overall, the evidence leaves me without substantial questions and doubts as to Applicant's eligibility and suitability for a security clearance. For all these reasons, I conclude Applicant has mitigated the security concerns arising from his handling protected information and personal conduct. *See* SEAD 4, App. A, ¶¶ 2(d) (1) through AG 2(d) (9).

Formal Findings

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

Paragraph 1, Guideline K:	FOR APPLICANT
Subparagraphs 1.a. through 1.c.:	For Applicant
Paragraph 2, Guideline E:	FOR APPLICANT
Subparagraph 2.a.:	For Applicant

Conclusion

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

ROBERT ROBINSON GALES
Administrative Judge