DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 22-00881
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Patricia Lynch-Epps, Esq., Department Counsel
For Applicant: Pro se

02/09/2024

_____

Decision

_____

OLMOS, Bryan J., Administrative Judge:

Applicant failed to mitigate the security concerns under Guideline K, Handling Protected Information and Guideline E, Personal Conduct. Eligibility for access to classified information is denied.

Statement of the Case

Applicant submitted a security clearance application (SCA) on September 9, 2021. On May 26, 2022, the Department of Defense (DOD) issued a Statement of Reasons (SOR) to Applicant detailing security concerns under Guideline K and Guideline E. The DOD issued the SOR under Executive Order (Exec. Or.) 10865, *Safeguarding Classified Information within Industry* (February 20, 1960), as amended; DOD Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (January 2, 1992), as amended (Directive); and the Security Executive Agent Directive 4 (SEAD 4), *National Security Adjudicative Guidelines* (AG), effective June 8, 2017.

Applicant submitted an answer to the SOR on June 16, 2022, and requested a decision based on the written record by an administrative judge, in lieu of a hearing. On

February 6, 2023, the DOD requested that Applicant supplement his answer by admitting or denying the specific allegations in the SOR, which he did on February 17, 2023.

On July 6, 2023, Department Counsel submitted the Government's File of Relevant Material (FORM), including Government's Exhibits (GX) 1 through 6. Applicant received the FORM on August 1, 2023. He did not provide a response to the FORM.

The case was assigned to me on November 6, 2023. The SOR and the Answer (GX 1-2) are the pleadings in the case. GX 3-6 are admitted without objection.

Findings of Fact

In his Answer, Applicant admitted SOR ¶¶ 1.a-1.c and 1.e. He denied ¶¶ 1.d, 1.f, 1.h, and 1.i, with explanations. He did not specifically admit or deny SOR ¶¶ 1.g or 2.a. As such, I will treat Applicant's lack of response to SOR ¶¶ 1.g and 2.a as a denial of those allegations. His SOR admissions are incorporated into my findings of fact. After a thorough and careful review of the pleadings and evidence submitted, I make the following additional findings of fact.

Applicant is 72 years old, married and has two adult children. He obtained his bachelor's degree in 1977. He started with the predecessor of his current employer in 1979 and has continuously remained in a full-time position with the company or its successor since then. As of his September 2021 SCA submission, he was a senior systems engineer. (GX 3, 5-6)

Employment records reflect that, from 2011 through 2020, Applicant committed multiple security violations that required reporting to the Government by his employer under 32 CFR Part 117.8 of the National Industrial Security Program Operating Manual (NISPOM). The first incident occurred in March 2011. (SOR ¶ 1.i) A company Individual Culpability Report (ICR) stated that company proprietary and competition-sensitive documents were left unsecured on Applicant's desk. Further inspection of Applicant's workspace yielded multiple unsecured proprietary documents. A security citation was issued to Applicant. (GX 4)

In August 2014 and again in November 2014, company proprietary documents were discovered unsecured in and around Applicant's desk and workspace. (SOR ¶¶ 1.g and 1.h) In both instances, an ICR was drafted and Applicant received security citations. (GX 4)

In September 2016, during a random building sweep, multiple company proprietary and export-controlled documents were discovered unsecured on Applicant's desk. (SOR ¶ 1.f) An ICR was drafted and Applicant received another security citation. (GX 4)

In two separate incidents in April 2018, Applicant's employer discovered that he left company proprietary and export-controlled documents and diagrams unsecured in his workspace. (SOR ¶¶ 1.d and 1.e) After the first incident, Applicant was specifically advised that "documents must be placed in a locked cabinet and the keys not accessible." After the second incident two weeks later, security personal requested that supervisors meet with Applicant to review company procedures regarding the protection of information. ICRs were issued in both instances. (GX 4)

In August 2018, during another random building sweep, company proprietary documents were discovered unattended and unsecured in Applicant's workspace. (SOR ¶ 1.c) An ICR was drafted and he received another security citation. It was noted that this was his third violation that year and security personal again advised supervisors to meet with him and take corrective measures. (GX 4)

During "routine monitoring of employee asset usage," company investigators observed that, from April through June 2020, Applicant sent four emails from his work email account to his personal email account that contained documents marked as company proprietary. (SOR ¶ 1.b) When confronted, Applicant stated that he sent the documents to his personal email so that he could work on them at home since "it was an inconvenience to pack up all his work assets to take home." An ICR was drafted and Applicant confirmed that he deleted the relevant files from his personal email and computer. He was advised of company policies regarding the use of personal email and received verbal counseling from his supervisor. (GX 4)

Despite the counseling, in August 2020, Applicant sent another document marked as proprietary and export controlled from his work email to his personal email. When confronted, Applicant stated that he sent the document to his personal email as a template for another work project and believed the document did not contain any proprietary information. However, his supervisor confirmed that the documents did contain proprietary information and that there was no "legitimate business purpose" for Applicant to have sent company "intellectual property" to his personal email. Another ICR was drafted. This was noted as Applicant's second "data infiltration incident" within the last 12 months and he was issued a written warning. (GX 4)

None of the reports reflect that there was ever a loss or compromise of classified information during any of these incidents and Applicant's supervisor noted that Applicant's actions were not "nefarious." When requested by his employer, he deleted the relevant documents from his personal email and home computer. (GX 4)

In his September 2021 SCA, Applicant disclosed that he was "written up" by his employer in April 2020 because he sent a document marked "company proprietary" from his work email to his personal email. He explained that everyone was remote working during the COVID pandemic and he was trying to complete an assignment to maintain the program schedule. Applicant blamed the "recent total encryption of all files" for making it "impossible" to work on any computer outside of the network. Applicant emphasized that he "CREATED" the document at issue and that "there was NOTHING

classified" in it. (Emphasis in original) He did not detail any of the other incidents in his SCA. (GX 3)

During his December 2021 background interview with a DOD investigator, Applicant again disclosed that he had received a written warning in April 2020. He described sending a document that he was drafting from his work computer to his personal email to continue working on the document. The investigator noted that Applicant "considered the document to be unclassified" and, at the time, was unaware that he was not allowed to send the document to his personal computer. He described later meeting with his supervisor about the incident and being required to review company policy on handling proprietary information. Afterwards, he claimed to understand the company policy and admitted his mistake. (GX 5)

Also during his background interview, Applicant stated that he had been employed with the company for over 40 years and that this was the "first incident of this nature that he had been involved in." He did not detail the other incidents or ICRs that he had received. (GX 5)

In his Answer, Applicant stated that he did not "completely admit fault nor deny culpability" regarding the incidents from 2011 through 2018. He stated that "[company] proprietary" was the "*de facto*" label for everything that came off the printer or that he worked with on the computer. He further stated that he was "always under the assumption" that he worked in a "safe and secure environment" and that no one was "allowed to graze through the offices and laboratories (without challenge) to examine and take what they wish." He also questioned company policy as he stated it was "peculiar" that his company defined "properly secure" as the use of "simple office locks." (Answer)

With regard to the incidents from April through August 2020, Applicant admitted the relevant allegations, but only discussed the incidents as a single event. He stated that, "as time became short," he sent documents to his personal email so that he could complete the task on time. He further stated that once he was notified of the error, he deleted the material from his home computer that day. (Answer)

Applicant did not respond to the FORM, so he did not provide any further information to explain or mitigate his actions.

Policies

It is well established that no one has a right to a security clearance. As the Supreme Court held in *Department of the Navy v. Egan*, "the clearly consistent standard indicates that security determinations should err, if they must, on the side of denials." 484 U.S. 518, 531 (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 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, 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. 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. Likewise, I have not drawn inferences grounded on mere speculation or conjecture.

Under Directive ¶ E3.1.14, the Government must present evidence to establish controverted facts alleged in the SOR. Under Directive ¶ E3.1.15, an "applicant is responsible for presenting witnesses and other evidence to rebut, explain, extenuate, or mitigate facts admitted by applicant or proven by Department Counsel and 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 the applicant may deliberately or inadvertently fail to safeguard classified information. Such decisions entail a certain degree of legally permissible extrapolation of potential, rather than actual, risk of compromise of classified information.

Analysis

Guideline K, Handling Protected Information

The security concern relating to the guideline 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.

Guideline K security concerns are not limited to violations of DOD rules and polices, but also encompass violations of industry rules and policies established for the protection of classified and sensitive information. *See* ISCR Case No. 15-08002 at 1 (App. Bd. July 17, 2018); ISCR Case No. 14-00963 at 3 (App. Bd. Jan. 13, 2015). Neither a violation of a specific rule nor an actual compromise of classified or sensitive information is required to establish a Guideline K concern if the conduct has security significance. *See* ISCR Case No. 11-05079 at 4-5 (App. Bd. Jun. 6, 2012); ISCR Case No. 20-00230 at 3 (App. Bd. Dec. 10, 2021).

AG ¶ 34 describes conditions that could raise a security concern and may be disqualifying. I have considered all of them, and the following are potentially applicable:

(b) collecting or storing protected information in any unauthorized location;

(c) loading, drafting, editing, modifying, storing, transmitting, or otherwise handling protected information, including images, on any unauthorized equipment or medium;

(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.

Applicant committed numerous security violations from 2011 through 2020 by repeatedly failing to secure protected information in an authorized location and forwarding proprietary work documents to his personal email in order to access those documents from his home computer. These actions were in violation of various rules established by his company in accordance with DOD policies and are of security significance. Although he was continually notified or counseled by his company's security team and management to secure sensitive information, the violations continued. AG ¶¶ 34(b), (c), (g), and (h) are established.

Once it is shown that an applicant has committed security violations, he or she has a "very heavy burden" in demonstrating mitigation. ISCR Case No. 14-05127 at 8 (App. Bd. June 24, 2016). An applicant's failure to accept responsibility for said violations will likely not meet the strict scrutiny standard of establishing reform or rehabilitation. *See* ISCR Case No. 14-05794 at 5 (App. Bd. July 7, 2016).

AG ¶ 35 describes conditions that could mitigate the security concerns and are potentially applicable:

(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 security violations span a period of over nine years, from 2011 to 2020. Although company records reflect numerous occasions where he received notification and counseling regarding the violations, there is no evidence in the record establishing that he fully recognized the significance of the violations or made substantive changes to how he managed sensitive information.

In his SCA and during his December 2021 background interview, Applicant only described a single "mistake" that he made in April 2020 when he sent work documents to his personal email. He claimed he was unaware of company policy when he sent the documents but had since reviewed and understood the policy. However, he then failed to address why he repeated the same violation just a few months later, in August 2020.

Instead, it is apparent that Applicant continually substituted his own assessment of the nature and security of the sensitive material he was handling over company policy. In discussing the April 2020 incident that he disclosed in his SCA, he emphasized that the document at issue was something he "CREATED" that had "NOTHING classified" in it. During his interview, he again stated that he considered the document to have nothing classified in it. In his Answer, he further stated disagreement with the company's definition of "properly secure," finding it "peculiar."

Applicant committed numerous security violations over an extended period. While some of those violations may have been unintentional, he has shown only limited recognition of the concerns or an ability to take substantive corrective action. These efforts fall short of his very heavy burden of persuasion as to mitigation. An additional violation occurring after Applicant's disclosed "mistake" in April 2020 undermines confidence that the violations are unlikely to recur. None of the above mitigating conditions are fully established.

Guideline E, Personal Conduct

AG ¶ 15 expresses the security concern regarding personal conduct:

> 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.

AG ¶ 16 describes conditions that could raise a security concern and may be disqualifying. I have considered all of them, and the following is potentially applicable:

> (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:
>
> > (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.

Applicant's mishandling of protected information is cross-alleged under Guideline E. That conduct reflects questionable judgment and an unwillingness to comply with rules and regulations. AG ¶ 16(d) is only partially applicable because the alleged conduct is sufficiently and explicitly covered for an adverse determination under Guideline K. However, the general concerns about questionable judgment and an unwillingness to comply with rules and regulations contained in AG ¶¶ 15 and 16(d) are established.

AG ¶ 17 describes conditions that could mitigate the security concerns and are potentially applicable:

> (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.

Applicant's multiple security violations that occurred over a nine-year span are not minor offenses nor did they occur under unique circumstances. The recency of his violations, including a violation in August 2020 after he recognized he made a "mistake" in April 2020, continue to cast doubt as to his trustworthiness, reliability and good judgment. AG ¶ 17(c) does not apply. Although he claimed to understand his company's policies, he has shown an inability or unwillingness to take corrective action. Applicant has not established that future security violations are unlikely to recur. AG ¶ 17(d) does 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 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 Guideline K and Guideline E in my whole-person analysis. Because Applicant requested a determination on the record without a hearing, I had no opportunity to evaluate his credibility and sincerity based on demeanor. *See* ISCR Case No. 01-12350 at 3-4 (App. Bd. Jul. 23, 2003).

Applicant has a long and established career with his employer. However, his poor management of proprietary information and his multiple security violations show a pattern of conduct lacking in security awareness. Additionally, by sending proprietary documents to his personal email, he substituted his judgment for that of company policy and prioritized work over security. Even though his actions were not "nefarious" in nature, they continue to raise doubts as to his trustworthiness, reliability, and judgment.

Overall, the record evidence leaves me with questions and doubts as to Applicant's eligibility and suitability for a security clearance. I conclude that Applicant failed to mitigate the handling protected information and personal conduct security concerns.

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.i:	Against Applicant
Paragraph 2, Guideline E:	AGAINST APPLICANT
Subparagraphs 2.a:	Against Applicant

Conclusion

It is not clearly consistent with the national interest to grant Applicant eligibility for a security clearance. Eligibility for access to classified information is denied.

_____
Bryan J. Olmos
Administrative Judge