DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 23-01001
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Aubrey M. De Angelis, Esq., Department Counsel
For Applicant: Todd A. Hull, Esq.

04/01/2025

_____

Decision

_____

TUIDER, Robert, Administrative Judge:

Applicant failed to mitigate security concerns arising under Guidelines K (handling protected information) and M (use of information technology); however, Guideline E (personal conduct) security concerns are mitigated as a duplication of the Guidelines K and M security concerns. Eligibility for access to classified information is denied.

Statement of the Case

On June 15, 2022, Applicant completed and signed an Electronic Questionnaires for Investigations Processing or security clearance application (SCA). (Government Exhibit (GE) 1) On September 8, 2023, the Defense Counterintelligence and Security Agency Consolidated Adjudication Services (DCSA) issued a statement of reasons (SOR) to Applicant. (Hearing Exhibit (HE) 2) This action was taken under Executive Order (Exec. Or.) 10865, *Safeguarding Classified Information within Industry*, February 20, 1960; DOD Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (Directive), January 2, 1992; and Security Executive Agent Directive 4, establishing in Appendix A the *National Security Adjudicative Guidelines for Determining Eligibility for Access to Classified Information or Eligibility to Hold a Sensitive Position* (AGs), effective June 8, 2017.

The SOR detailed reasons why the DCSA notified Applicant that it intended to deny or revoke his security clearance because it did not find that it is clearly consistent with the interests of national security to grant or continue a security clearance for him. Specifically, the SOR set forth security concerns arising under Guidelines K, M, and E. (Hearing Exhibit (HE) 2) On November 8, 2023, Applicant responded to the SOR. (HE 3)

On February 8, 2024, Department Counsel was ready to proceed. On February 20, 2024, the case was assigned to me. On March 1, 2024, DOHA issued a notice of hearing, scheduling the hearing for April 5, 2024. (HE 1) Applicant's hearing was held as scheduled.

At his hearing, Department Counsel offered three exhibits, and Applicant offered five exhibits. (Tr. 16-17; GE 1-3; Applicant Exhibit (AE) A-AE E) All proffered exhibits were admitted into evidence without objection. (Tr. 16,18) The record was held open after the hearing until April 12, 2024. (Tr. 90-91) On April 8, 2024, Applicant provided one post-hearing exhibit. (AE F) All proffered exhibits were admitted into evidence without objection. (Tr. 16,18; AE F) On April 19, 2024, DOHA received a transcript of Applicant's security clearance hearing.

Some details were excluded to protect Applicant's right to privacy. Specific information is available in the cited exhibits and transcript.

Findings of Fact

Applicant admitted the factual support for the allegations in SOR ¶¶ 1.a, 2.a, and 3.a. (HE 3) He denied that the facts established a disqualifying security concern. He provided clarifications, extenuating, and mitigating information. (HE 3)

Applicant is a 64-year-old senior communications systems engineer who has been employed by the current DOD contractor since June of 2022. (Tr. 36-37, 45) He graduated from high school in 1978. (Tr. 37-38) In 1984, he received a bachelor's degree with a major in electrical engineering from a university, and in 1990, he received a master's degree in electrical engineering. (Tr. 39-40) DOD contractors have employed him since 1992. (Tr. 47, 64, 76) In 1996, he married, and his son is 17 years old. (Tr. 40-41) His spouse has worked for a U.S. Government agency since 2001. (Tr. 43) He did not serve in the U.S. military. (Tr. 44) He seeks a security clearance to enhance his position and responsibilities with his current employer. (Tr. 45, 62) His resume provides further details about his professional background and experience. (AE A)

Handling protected information, use of information technology, and personal conduct

SOR ¶ 1.a alleges a handling protected information security concern. In July 2018, Applicant connected his personal thumb drive to a DOD contractor's Intranet in violation of the DOD contractor's policy. Over a two-day period, he downloaded U.S. Government-owned data classified as Export Controlled Information/For Official Use Only to his thumb drive. The data included software code for a program on which he had been working. By

downloading this information, he violated the program's non-disclosure agreement, which he had signed. The DOD contractor determined that he is not eligible for rehire.

SOR ¶¶ 2.a and 3.a cross allege the information in SOR ¶ 1.a as use of information technology and personal conduct security concerns, respectively.

Applicant worked for the DOD contractor from 2016 to July 2018 as a communications systems engineer. (Tr. 49, 64) He received an outstanding performance review in July of 2018. (Tr. 49; AE B) He held a security clearance when he used a thumb drive to access the DOD contractor's Intranet. (Tr. 50)

Applicant did considerable work on codes for his employer. (Tr. 53) One project he worked on for the DOD contractor, starting in 2017, was called Z. (Tr. 65) Applicant worked on Z full time for one year, and he spent all of his time coding and researching. (Tr. 65, 69) He received excellent comments from a supervisor for his work on the Z team. (AE B) He wanted to change employment and move to a different state. (Tr. 52) Many other contractor employees worked on Z too; however, only three or four people worked on Z in the open area. (Tr. 66) He realized he could not remember the data and codes, and he decided to keep a copy of them. (Tr. 53) He downloaded the material after he submitted a resignation letter to his employer. (Tr. 54, 76, 78) He already had an offer of employment from another DOD contractor. (Tr. 58) The contractor said the download of the Z program could have compromised two years of work; however, Applicant said he believed it may be only one year of work. (Tr. 69) The contractor said the download contained the code "for the entire end to end simulation of the system." (Tr. 70) Applicant acknowledged he made a mistake when he downloaded the codes onto his thumb drive. (Tr. 53)

Applicant signed a nondisclosure agreement; however, he did not remember whether it discussed using thumb drives. (Tr. 66-67) He understood that he was not allowed to use a personal thumb drive to store information at work. (Tr. 67) A company thumb drive can be used to transport or store information when an employee is traveling. (Tr. 68)

Applicant said the data he downloaded was based on commercially available papers. (Tr. 54) He downloaded the information in an open area and not in a sensitive compartmented information facility (SCIF). (Tr. 56) The information he downloaded was unclassified. (Tr. 54) He downloaded PowerPoint briefings, details of algorithms, and papers implementing algorithms and codes. (Tr. 68) He suggested the documents might have been marked, "For Official Use Only (FOUO)"; however, he did not specifically remember the markings on the documents. (Tr. 69) He did not realize the information was proprietary. (Tr. 55) He downloaded the information on a weekend to enable him to reference the information in the future. (Tr. 55, 77) He said he was foolish to think the information was not proprietary. (Tr. 56) He brought the thumb drive home, and he did not think he put the thumb drive into a computer at home. (Tr. 72) He was very remorseful about what he had done. (Tr. 56, 63) He said he did not share the information contained on the thumb drive. (Tr. 56) He provided the thumb drive to his employer when the security

infraction was investigated. (Tr. 57) He cooperated with the investigation of the security infraction. (Tr. 57)

Applicant received extensive security training over the years from various DOD contractors. (Tr. 58) He said he was advised not to download classified information onto a personal thumb drive. (Tr. 59) He did not have incidents before July 2018 in which he mishandled or improperly downloaded information. (Tr. 59) He promised not to commit the error in judgment in the future. (Tr. 59-60) He believes he is ready to regain access to classified information. (Tr. 61)

Around 2019, Federal Bureau of Investigation (FBI) agents interviewed him many times. (Tr. 75) After about 2019, the FBI did not contact him. (Tr. 75) He denied that he was engaging in espionage, and he stated he lacked an intention to harm his employer. (Tr. 77) There is no evidence anyone paid Applicant to steal the proprietary information from his employer.

Character Evidence

Applicant's friend and coworker has known Applicant for 19 years. (Tr. 20, 24) Another friend and coworker has known him for 17 years. (AE D) The general sense of their statements is that Applicant is diligent, trustworthy, reliable, and professional. (Tr. 20-23; AE D) He is loyal to the U.S. Government. (Tr. 20-23; AE D) He has good judgment and is an asset to the government. (Tr. 23-24)

Applicant's supervisor from 2020 to 2022 described him as intelligent, competent, reliable, professional, trustworthy, and conscientious about protection of classified information. (Tr. 27-32; AE D) The SOR allegation is inconsistent with the behavior his supervisor observed. (Tr. 33) He recommended reinstatement of Applicant's security clearance. (Tr. 34-35)

Applicant's performance evaluations indicate he met or exceeded expectations. (Tr. 46, 48; AE E; AE F) In 2023, he received a 2023 Team Achievement Award from his employer. (Tr. 46-47; AE C)

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." *Id*. at 527. The President has authorized the Secretary of Defense or his designee to grant applicant's 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.

Eligibility for a security clearance is predicated upon the applicant meeting the criteria contained in the adjudicative guidelines. These guidelines are not inflexible rules of law. Instead, recognizing the complexities of human behavior, these guidelines are applied in conjunction with an evaluation of the whole person. An administrative judge's overarching adjudicative goal is a fair, impartial, and commonsense decision. An administrative judge must consider all available, reliable information about the person, past and present, favorable and unfavorable.

The Government reposes a high degree of trust and confidence in persons with access to classified information. This relationship transcends normal duty hours and endures throughout off-duty hours. 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 about potential, rather than actual, risk of compromise of classified information. 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 it is based, in whole or in part, on any express or implied determination about applicant's allegiance, loyalty, or patriotism. It is merely an indication the applicant has not met the strict guidelines the President, Secretary of Defense, and DNI have established for issuing a clearance.

Initially, the Government must establish, by substantial evidence, conditions in the personal or professional history of the applicant that may disqualify the applicant from being eligible for access to classified information. The Government has the burden of establishing controverted facts alleged in the SOR. *See Egan*, 484 U.S. at 531. "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 Directive presumes there is a nexus or rational connection between proven conduct under any of the Guidelines and an applicant's security eligibility. Direct or objective evidence of nexus is not required." ISCR Case No. 18-02581 at 4 (App. Bd. Jan. 14, 2020) (citing ISCR Case No. 15-08385 at 4 (App. Bd. May 23, 2018)).

Once the Government establishes a disqualifying condition by substantial evidence, the burden shifts to the applicant to rebut, explain, extenuate, or mitigate the facts. Directive ¶ E3.1.15. An applicant "has the ultimate burden of demonstrating that it is clearly consistent with the national interest to grant or continue his [or her] security clearance." ISCR Case No. 01-20700 at 3 (App. Bd. Dec. 19, 2002). 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). "[S]ecurity clearance determinations should err, if they must, on the side of denials." *Egan*, 484 U.S. at 531; *see* AG ¶ 2(b).

Analysis

Handling Protected Information and Use of Information Technology

AG ¶ 33 describes the handling protected information security 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.

AG ¶ 39 describes the use of information technology security concern:

> Failure to comply with rules, procedures, guidelines, or regulations pertaining to information technology systems may raise security concerns about an individual's reliability and trustworthiness, calling into question the willingness or ability to properly protect sensitive systems, networks, and information. Information Technology includes any computer-based, mobile, or wireless device used to create, store, access, process, manipulate, protect, or move information. This includes any component, whether integrated into a larger system or not, such as hardware, software, or firmware, used to enable or facilitate these operations.

AG ¶ 34 describes the security concern for handling protected information security concerns as follows:

> (a) deliberate or negligent disclosure of protected information to unauthorized persons, including, but not limited to, personal or business contacts, the media, or persons present at seminars, meetings, or conferences;
>
> (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;
>
> (d) inappropriate efforts to obtain or view protected information outside one's need to know;
>
> (e) copying or modifying protected information in an unauthorized manner designed to conceal or remove classification or other document control markings;
>
> (f) viewing or downloading information from a secure system when the information is beyond the individual's need-to-know;

(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 ¶ 40 lists conditions that could raise a use of information technology security concern and may be disqualifying as follows:

(a) unauthorized entry into any information technology system;

(b) unauthorized modification, destruction, or manipulation of, or denial of access to, an information technology system or any data in such a system;

(c) use of any information technology system to gain unauthorized access to another system or to a compartmented area within the same system;

(d) downloading, storing, or transmitting classified, sensitive, proprietary, or other protected information on or to any unauthorized information technology system;

(e) unauthorized use of any information technology system;

(f) introduction, removal, or duplication of hardware, firmware, software, or media to or from any information technology system when prohibited by rules, procedures, guidelines, or regulations or when otherwise not authorized;

(g) negligence or lax security practices in handling information technology that persists despite counseling by management; and

(h) any misuse of information technology, whether deliberate or negligent, that results in damage to the national security.

The record establishes AG ¶¶ 34(b), 34(c), 34(g), 40(d), 40(e), and 40(f). Additional discussion is in the mitigation section, *infra*.

AG ¶ 35 lists conditions that could mitigate handling protected information security concerns:

(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.

AG ¶ 41 lists conditions that could mitigate use of information technology security concerns as follows:

(a) so much time has elapsed since the behavior happened, or it happened under such unusual circumstances, that it is unlikely to recur and does not cast doubt on the individual's reliability, trustworthiness, or good judgment;

(b) the misuse was minor and done solely in the interest of organizational efficiency and effectiveness;

(c) the conduct was unintentional or inadvertent and was followed by a prompt, good faith effort to correct the situation and by notification to appropriate personnel; and

(d) the misuse was due to improper or inadequate training or unclear instructions.

In ISCR Case No. 10-04641 at 4 (App. Bd. Sept. 24, 2013), the DOHA Appeal Board explained Applicant's responsibility for proving the applicability of mitigating conditions as follows:

> Once a concern arises regarding an Applicant's security clearance eligibility, there is a strong presumption against the grant or maintenance of a security clearance. *See Dorfmont v. Brown*, 913 F. 2d 1399, 1401 (9th Cir. 1990), *cert. denied*, 499 U.S. 905 (1991). After the Government presents evidence raising security concerns, the burden shifts to the applicant to rebut or mitigate those concerns. *See* Directive ¶ E3.1.15. The standard applicable in security clearance decisions is that articulated in *Egan*, *supra*. "Any doubt concerning personnel being considered for access to classified information will be resolved in favor of the national security." Directive, Enclosure 2 ¶ 2(b).

None of the mitigating conditions are fully established. In July 2018, Applicant connected his personal thumb drive to a DOD contractor's Intranet in violation of the DOD contractor's policy. During a weekend, he downloaded contractor-owned data relating to project Z, classified as Export Controlled Information/For Official Use Only, to his personal

thumb drive. The data included software code on which he had been working extensively for one year. By downloading this information, he indicated an intent to violate the program's non-disclosure agreement, which he had signed. The DOD contractor determined that he is not eligible for rehire.

Applicant was in the process of changing employment and moving to a different state. In addition to Applicant, two or three other employees worked on Z in the open area. Applicant downloaded the material after he submitted a resignation letter to his employer. He already had an offer of employment from another DOD contractor. The download of the Z program could have compromised about one year of work on project Z. The contractor said the download contained the code "for the entire end to end simulation of the system." (Tr. 70)

Applicant did not provide a credible non self-serving reason for downloading valuable information from his employer's internet. Poor judgment is shown when he downloaded proprietary information shortly before leaving employment. Applicant might violate employer's rules if he decides it is personally advantageous for him to do so. His decision to download the proprietary information casts doubt on his reliability, trustworthiness, and judgment. Handling protected information and use of information technology security concerns are not mitigated.

Personal Conduct

AG ¶ 15 describes the personal conduct security concern as follows:

> 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 information. Of special interest is any failure to provide truthful and candid answers during the security clearance process or any other failure to cooperate with the security clearance process. . . .

AG ¶ 16 lists personal conduct disqualifying conditions that are potentially relevant in this case as follows:

> (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;
>
> (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; and

(e) personal conduct, or concealment of information about one's conduct, that creates a vulnerability to exploitation, manipulation, or duress by a foreign intelligence entity or other individual or group. Such conduct includes: (1) engaging in activities which, if known, could affect the person's personal, professional, or community standing.

None of the personal conduct disqualifying conditions apply. The allegation in SOR ¶ 1.a was cross alleged in SOR ¶ 3.a. The conduct in SOR ¶ 3.a is addressed under the handling protected information and use of information technology guidelines. Essentially this allegation is a duplication. His conduct under the two guidelines is disqualifying. The FBI and security officials are aware of the conduct in SOR ¶ 3.a, and he is not a vulnerable to exploitation, manipulation, or duress by a foreign intelligence entity or other individual or group. Personal conduct security concerns are refuted.

Whole-Person Analysis

In all adjudications, the protection of our national security is the paramount concern. A careful weighing of several variables in considering the whole-person concept is required, including the totality of his or her acts, omissions, and motivations. Each case is decided on its own merits, taking into consideration all relevant circumstances, and applying sound judgment, mature thinking, and careful analysis. Under the whole-person concept, 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), "[t]he 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. My comments under Guidelines K, M, and E are incorporated in my whole-person analysis. Some of the factors in AG ¶ 2(d) were addressed under those guidelines but some warrant additional comment.

Applicant is a 64-year-old senior communications systems engineer who has been employed by the current DOD contractor since June of 2022. In 1984, he received a bachelor's degree with a major in electrical engineering from a university, and in 1990, he received a master's degree in electrical engineering. DOD contractors have employed him since 1992. His resume provides further details about his professional background and experience.

The general sense of two friends and coworkers' statements is that Applicant is diligent, trustworthy, reliable, and professional. He is loyal to the U.S. Government, has good judgment, and is an asset to the government. His supervisor from 2020 to 2022 described him as intelligent, competent, reliable, professional, trustworthy, and conscientious about protection of classified information. The SOR allegation is inconsistent with the behavior his supervisor observed. He recommended reinstatement of Applicant's security clearance. Applicant's performance evaluations indicate he met or exceeded expectations. In 2023, he received a 2023 Team Achievement Award from his employer.

The reasons for denial of his security clearance are more persuasive. Those reasons are discussed in the analysis for Guidelines K and M, *supra*.

It is well settled that once a concern arises regarding an applicant's security clearance eligibility, there is a strong presumption against granting a security clearance. *See Dorfmont*, 913 F. 2d at 1401. "[A] favorable clearance decision means that the record discloses no basis for doubt about an applicant's eligibility for access to classified information." ISCR Case No. 18-02085 at 7 (App. Bd. Jan. 3, 2020) (citing ISCR Case No. 12-00270 at 3 (App. Bd. Jan. 17, 2014)).

I have carefully applied the law, as set forth in *Egan*, Exec. Or. 10865, the Directive, the AGs, and the Appeal Board's jurisprudence to the facts and circumstances in the context of the whole person. Guideline E (personal conduct) security concerns are mitigated; however, Guidelines K (handling protected information) and M (use of information technology) security concerns are not mitigated.

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
Subparagraph 1.a:	Against Applicant

Paragraph 2, Guideline M:	AGAINST APPLICANT
Subparagraph 2.a:	Against Applicant
Paragraph 3, Guideline E:	FOR APPLICANT
Subparagraph 3.a:	Against Applicant

Conclusion

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

_____
Robert Tuider
Administrative Judge