DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 20-03319
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Andrew H. Henderson, Esq., Department Counsel
For Applicant: *Pro se*

11/10/2022

_____

Decision

_____

HARVEY, Mark, Administrative Judge:

Guidelines K (handling protected information) and Guideline E (personal conduct) security concerns are not mitigated. Eligibility for access to classified information is denied.

Statement of the Case

On January 21, 2019, Applicant completed an Electronic Questionnaires for Investigations Processing or security clearance application (SCA). (Government Exhibit (GE) 1) On March 25, 2022, the Defense Counterintelligence and Security Agency (DCSA) Consolidated Adjudications Facility (CAF) issued a statement of reasons (SOR) to Applicant under Executive Order (Exec. Or.) 10865, *Safeguarding Classified Information within Industry* (February 20, 1960); Department of Defense (DOD) Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (Directive) (January 2, 1992), as amended; 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. (Hearing Exhibit (HE) 2)

The SOR detailed reasons why the DCSA CAF did not find under the Directive that it is clearly consistent with the interests of national security to grant or continue a security clearance for Applicant and recommended referral to an administrative judge to determine whether a clearance should be granted, continued, denied, or revoked. Specifically, the SOR set forth security concerns arising under Guidelines K and E. (HE

2) On March 29, 2022, Applicant responded to the SOR, and she requested a decision based on the written record. (HE 3) On July 6, 2022, Department Counsel requested a hearing.

On July 6, 2022, Department Counsel was ready to proceed. On July 21, 2022, the case was assigned to me. On August 15, 2022, the Defense Office of Hearings and Appeals issued a Notice setting the hearing for September 12, 2022. (HE 1A) Applicant did not receive the government exhibits, and the hearing was rescheduled. On September 15, 2022, DOHA issued a Notice setting the hearing for October 21, 2022. (HE 1B) Applicant's hearing was held as rescheduled on October 21, 2022, in the vicinity of Arlington, Virginia using the Microsoft Teams video teleconference system.

During the hearing, Department Counsel offered seven exhibits, and all proffered exhibits were admitted into evidence without objection. (Tr. 14-17; GE 1-GE 7) Applicant did not offer any documents at her hearing. On October 31, 2022, DOHA received a copy of the transcript.

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

Findings of Fact

In Applicant's SOR response, she admitted the SOR allegation in ¶ 2.c. (HE 3) She denied the SOR allegations in SOR ¶¶ 1.a through 1.f, 2.a, and 2.b. She also provided mitigating information. Her admissions are accepted as findings of fact.

Applicant is a 48-year-old employee of a DOD contractor. (Tr. 6) She continuously worked for the DOD contractor, a large corporation, for 22 ½ years. (Tr. 8) She worked for the DOD contractor as a laboratory technician, crane operator, uniform security officer, and industrial security officer. (Tr. 8, 19) She was an industrial security officer for 13 years from 2006 to 2019. (Tr. 9) She held a security clearance for all of her employment with the DOD contractor, except for the last three years. (Tr. 8) Applicant did not submit any performance evaluations or character letters attesting to her honesty, trustworthiness, reliability, or attention to detail.

In 1992, Applicant graduated from high school. (Tr. 6) In 1997, she earned a bachelor's degree in park and land management and criminal justice. (Tr. 7) She honorably served in the Army from 1997 to 1998, and she received an early discharge due to pregnancy. (Tr. 7, 19) After her discharge, she had a miscarriage. (Tr. 19) She was married the first time from 1997 to 1998, and the second time from 2007 to present. (Tr. 7) She does not have any children. (Tr. 7)

Handling Protected Information and Personal Conduct

SOR ¶ 1.a alleges in about July 2019, Applicant failed to have a security professional inspect the property she was moving out of the sensitive compartmented information facility (SCIF).

After the counseling in March 2019 for failing to double wrap classified or sensitive materials, Applicant asked to be transferred out of industrial security to a laboratory and then to a range to be a crane operator. (Tr. 27-28) She wanted to be transferred because there was too much work and stress in industrial security. (Tr. 28) She retained her desk in the SCIF because the job as a crane operator was potentially temporary, and she may have needed to return to her industrial security duties. (Tr. 32)

A coworker reported Applicant's possession of two books which security officials believed might show a foreign influence connection to Russia. (Tr. 34) Applicant's desk in the SCIF had a book about a Russian espionage case from the World War II era that a former security manager gave her and a 1980s book about translations from Russian to English that she received from a coworker. (Tr. 29-32; GE 4) Security officials said a book about Russian spies and how to encrypt writing was found on Applicant's desk between March 2019 and April 2019. (GE 5 at 2) Concerns about the Russian connection caused security to lock Applicant out of the SCIF. (*Id*.) Security officials alleged that she gained unauthorized access to the SCIF; she wiped her computer when she performed a manual backup; and she removed two boxes and a five-gallon bucket containing property from the SCIF without security inspecting the boxes or bucket. (Tr. 38; GE 5 at 2) She was asked to bring the items back, and she brought one box and explained the other items were food storage. (*Id*.)

Applicant said a person working in the SCIF told her to clear out her desk in the SCIF because she had moved to a different location. (Tr. 37; GE 2 at 19) On July 24, 2019, she collected most of her personal items, such as papers and books, put the items in boxes, and moved them out of the SCIF. (Tr. 37; GE 2 at 20) She placed the items in her car. (Tr. 46) She said no one was in the SCIF when she removed her property. (Tr. 46) She believed security personnel discovered she removed her items from the SCIF because it was on video. (Tr. 46) When Applicant was asked about removing her property from the SCIF, she admitted it. (Tr. 46) Eight days after she removed the property from the SCIF, she said she returned the property for security's inspection. (Tr. 47; GE 2 at 10) They did not find any prohibited items in the property she returned for inspection. (Tr. 47; GE 2 at 21)

Applicant was unaware of any regulation or rule requiring security to inspect items being removed from the SCIF; however, she admitted that two people were supposed to check furniture being removed from the SCIF and the items being removed when someone retired or was terminated. (Tr. 37-38, 44; GE 2 at 20) She denied that she "piggy-backed" or followed another employee into the SCIF. (Tr. 37-38, 48-49) She said she used her badge to gain access to the SCIF. (Tr. 38, 48-49) Two days after she retrieved her items from the SCIF, she went back to the SCIF to retrieve more of her personal property, and her badge would not open the door. (Tr. 49) She was not told at that point that she did not have access to the SCIF. (Tr. 49) She attempted to back up her desktop computer in the SCIF, and she was unable to do it. (Tr. 38) She said she called the help desk for assistance. (Tr. 38) She denied that she knew how to wipe her computer. (Tr. 40) She said there are cameras throughout the SCIF, and it would be stupid for her to do something inside the SCIF that was a security violation. (Tr. 41) Applicant believes two coworkers conspired against her and made up the allegations in

SOR ¶ 1.a. (GE 2 at 23) The file does not contain any statements from the two employees or from security officials with personal knowledge about: when she was locked out of the SCIF; when she was told that her access to the SCIF was terminated; or whether she was alone in the SCIF when her computer was wiped and the property was removed from the SCIF.

SOR ¶¶ 1.b and 1.c allege in about January and March 2019, Applicant failed to follow procedures for wrapping and mailing classified or sensitive program material. Applicant's July 18, 2019 Office of Personnel Management (OPM) personal subject interview (PSI) states in late 2018 and March 2019, she failed to double wrap packages containing classified or sensitive program material. (Tr. 24; GE 2 at 12; GE 7) Classified and sensitive papers are supposed to be placed inside one envelope, and that envelope is then placed inside another envelope. (Tr. 42) The party receiving the improperly wrapped packages promptly reported the rule violation. Applicant admitted she mailed both packages, and she believes she was verbally counseled about both packages on the same date. (Tr. 24-25) She frequently sent documents through the mail, and she knew how to package classified and sensitive materials. (Tr. 42) She acknowledged she made a mistake in her packaging of the materials. (Tr. 25) She was overworked, and she suggested she was distracted and overlooked the correct packaging of the materials. (Tr. 42-43) There was no compromise of classified information. (GE 7)

SOR ¶ 1.d alleges in about April 2013, Applicant failed to report her handling of materials for which she did not have access. Applicant's July 18, 2019 OPM PSI states she "opened a package [she] was not cleared for"; however, the contractor's record did not confirm this security violation. (GE 2 at 12) In her SOR response, Applicant said she opened a package that did not have any markings, and she discovered she was not cleared for the material inside the package. She sealed the package; she placed it into the safe; and she informed her supervisor. (SOR response) The package was returned to the sender. (*Id*.) She received a correction action memo (CAM) for the incident; however, she believes it was unfair because she had no way of knowing she was not cleared for the material until she opened the package. (*Id*.)

SOR ¶ 1.e alleges in September 2019, Applicant presented two classified program refresher briefings to an employee who did not have access. For classified briefings, they read the same information to the employee, except the name of the program is different for each program. (Tr. 43) Applicant said the incident occurred in 2013. In 2013, Applicant was counseled either verbally or with a CAM for a security violation because she briefed someone on the wrong program. (Tr. 22-23; GE 2 at 12; GE 3; GE 6) There was no evidence that the improper briefing occurred in September 2019.

SOR ¶ 1.f alleges in about July 2019, Applicant was debriefed from all access to the building containing the SCIF because of the security violations in SOR ¶¶ 1.a through 1.e. Applicant said she was told that she was debriefed because her work in the SCIF was not needed due to her transfer to work at a range in another location. (Tr. 34-35) In February 2020, she learned she was debriefed at least in part because of the allegations in SOR ¶¶ 1.a, 1.b, and 1.c. (Tr. 36)

SOR ¶ 2.a cross alleges the information in SOR ¶ 1 under the personal conduct guideline. SOR ¶ 2.b cross alleges the information in SOR ¶¶ 1.a through 1.c. SOR ¶ 2.c alleges that Applicant received two corrective action memos from about September 2012 to about April 2013 for the conduct alleged in SOR ¶¶ 1.d and 1.e.

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, *Safeguarding Classified Information within Industry* § 2 (Feb. 20, 1960), as amended.

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 Director of National Intelligence 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 guidelines presume a nexus or rational connection between proven conduct under any of the criteria

listed therein and an applicant's security suitability. *See* ISCR Case No. 95-0611 at 2 (App. Bd. May 2, 1996).

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

AG ¶ 33 articulates the security concern for handling protected information:

> 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 ¶ 34 lists conditions that could raise a security concern and may be disqualifying in this case:

> (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.

In July 2019, Applicant's access to the SCIF was blocked or suspended because some materials were found on her desk, which security officials erroneously believed raised a Russia-related foreign-influence concern. Those Russia-related materials do not raise a valid concern that she is a Russian agent. She obtained access to the SCIF, wiped her hard drive on her computer, and removed two boxes and a five-gallon bucket of materials without having them inspected. SOR ¶ 1.a is substantiated because she should not have removed materials from the SCIF after her access was revoked unless she was escorted by a cleared person. AG ¶ 34(g) is established by substantial evidence.

SOR ¶¶ 1.b and 1.c allege, and Applicant admitted that in 2019 she improperly wrapped classified material for mailing on two occasions. AG ¶ 34(g) is established by substantial evidence.

SOR ¶ 1.d alleges in about April 2013, Applicant failed to report her handling of materials for which she did not have access. The only evidence of this allegation is the OPM PSI, and it does not say she failed to report the opening of a package for which she was not cleared. Applicant said she opened an unmarked package, discovered she was not cleared to access the information, and she reported the incident to her supervisor. SOR ¶ 1.d is refuted.

SOR ¶ 1.e alleges, and Applicant admitted that she improperly briefed someone about a program. She said she should have verified that she had the correct program for the briefing. SOR ¶ 1.e indicates this rule violation occurred in 2019 and the evidence is that it occurred in 2013. SOR ¶ 1.e is substantiated. AG ¶¶ 34(a) and 34(g) apply to this violation of the rules.

SOR ¶ 1.f alleges, and Applicant admitted that she was debriefed from access to the SCIF in July 2019 for the conduct alleged in SOR ¶¶ 1.a through 1.e. There is no allegation in ¶ 1.f that Applicant did anything that implicates any security concern. SOR ¶ 1.f alleges an administrative action by security officials and not an improper or inappropriate action by Applicant. SOR ¶ 1.f is refuted.

AG ¶ 35 lists conditions that could mitigate security concerns including:

(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.

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).

Applicant improperly briefed someone about a program in 2013. She ensured this mistake was not repeated. AG ¶ 35(a) applies to this rule violation. SOR ¶ 1.e is mitigated.

Applicant improperly packaged two items for mailing in 2019. This rule violation was inadvertent; the party receiving the mail promptly reported the improper packaging; there is no evidence of compromise; and it does not suggest a pattern. AG ¶ 35(d) applies to these two rule violations. SOR ¶¶ 1.b and 1.c are mitigated.

Applicant had the burden of proving that she properly accessed the SCIF after security blocked her access. She did not provide any witness statements from security or her supervisor that she was unaware her access to the SCIF was blocked or terminated. She said there are cameras in the SCIF, and she believed that is how her access was discovered. She said no one was in the SCIF when she was there removing her property. She did not provide a statement from an impartial person who reviewed the videotape supporting her description of how she obtained access to the SCIF. She did not meet her burden of proving she properly accessed the SCIF. The security record indicates she wiped her hard drive on her computer in the SCIF. Applicant denied that she wiped her hard drive, and she said she sought assistance from the help desk to back up her computer. She did not provide a statement from the information technology office

supporting her claim that she sought help with backing up her hard drive and the erasure of the information on her hard drive was accidental. She failed to meet her burden of proof. None of the mitigating conditions fully apply to accessing the SCIF, erasing the hard drive on her computer in the SCIF, and removing property from the SCIF. Handling protected information security concerns are not mitigated.

Personal Conduct

AG ¶ 15 explains why personal conduct is a security concern stating:

> 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. . . .

AG ¶ 16 includes two conditions that could raise a security concern and may be disqualifying include:

> (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.

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

Applicant's entry of the SCIF after she was blocked, erasure of the hard drive of the computer in the SCIF, and removal of property from the SCIF are discussed in the previous section. This information is damaging to her personal, professional, and community standing. AG ¶ 16(e) is established.

AG ¶ 17 provides seven conditions that could mitigate security concerns in this case:

> (a) the individual made prompt, good-faith efforts to correct the omission, concealment, or falsification before being confronted with the facts;
>
> (b) the refusal or failure to cooperate, omission, or concealment was caused or significantly contributed to by advice of legal counsel or of a person with professional responsibilities for advising or instructing the individual specifically concerning security processes. Upon being made aware of the requirement to cooperate or provide the information, the individual cooperated fully and truthfully;
>
> (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;
>
> (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;
>
> (e) the individual has taken positive steps to reduce or eliminate vulnerability to exploitation, manipulation, or duress;
>
> (f) the information was unsubstantiated or from a source of questionable reliability; and
>
> (g) association with persons involved in criminal activities was unwitting, has ceased, or occurs under circumstances that do not cast doubt upon the individual's reliability, trustworthiness, judgment, or willingness to comply with rules and regulations.

None of the mitigating conditions fully apply. Applicant denied that she was aware that her access to the SCIF was revoked. She denied that she wiped the hard drive of the computer in the SCIF. She said the property she removed from the SCIF was all personal property. See discussion in previous section. She did not take full responsibility for her

actions. None of the mitigating conditions fully apply to Applicant's conduct. Personal conduct security concerns are not 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 the Applicant's conduct and all the 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), "[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 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 48-year-old employee of a DOD contractor. She continuously worked for her current employer, a large corporation, for 22 ½ years. She worked for the DOD contractor as a laboratory technician, crane operator, uniform security officer, and industrial security officer. She was an industrial security officer for 13 years from 2006 to 2019. She held a security clearance for all of her employment with the DOD contractor, except for the last three years. In 1997, Applicant earned a bachelor's degree in park and land management and criminal justice. She honorably served in the Army from 1997 to 1998.

The evidence against granting access to classified information is more persuasive. In July 2019, Applicant's access to the SCIF was blocked; however, she accessed the SCIF without having an escort. She wiped the hard drive on her computer in the SCIF, and she removed property from the SCIF without having the property inspected. She denied that her access to the SCIF was blocked and that she purposely wiped the hard drive. She said the property she removed from the SCIF was her own personal property. She has not taken responsibility for her violation of the rules in the SCIF in July 2019.

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. Applicant failed to mitigate 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
Subparagraph 1.a:	Against Applicant
Subparagraphs 1.b through 1.f:	For Applicant
Paragraph 2, Guideline E:	AGAINST APPLICANT
Subparagraph 2.a:	For Applicant
Subparagraph 2.b:	Against Applicant
Subparagraph 2.c:	For Applicant

Conclusion

I conclude that it is not clearly consistent with the interests of national security of the United States to grant or continue Applicant's national security eligibility for access to classified information. Eligibility for access to classified information is denied.

_____
Mark Harvey
Administrative Judge