DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 24-01586
	)	
Applicant for Security Clearance	)	

Appearances

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

05/20/2025

Decision

HARVEY, Mark, Administrative Judge:

Applicant mitigated security concerns arising under Guidelines E (personal conduct), K (handling protected information), and M (information technology systems). Eligibility for access to classified information is granted.

Statement of the Case

On October 27, 2022, Applicant completed and signed an Electronic Questionnaires for Investigations Processing or security clearance application (SCA). (Government Exhibit (GE) 1) On October 16, 2024, the Defense Counterintelligence and Security Agency (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. (Hearing Exhibit (HE) 2)

The SOR detailed reasons why the DCSA notified Applicant that it intended to deny or revoke her security clearance. Specifically, the SOR set forth security concerns arising under Guidelines E, K, and M. (Hearing Exhibit (HE) 2) On October 26, 2024, Applicant provided her response to the SOR, and she requested a decision based on the written record without a hearing before an administrative judge. (HE 3)

On December 19, 2024, Department Counsel requested a hearing. On January 15, 2025, the case was assigned to me. I granted the request for a hearing. On January 21, 2025, DOHA issued a notice of hearing, scheduling the hearing for February 27, 2025. (HE 1) Applicant's hearing was held as scheduled.

At her hearing, Department Counsel offered seven exhibits, and Applicant offered one exhibit. (Tr. 26-28; GE 1-7; Applicant Exhibit (AE) A) All proffered exhibits were admitted into evidence without objection. (Tr. 26-28) On March 10, 2025, DOHA received a transcript of Applicant's security clearance hearing. The record was held open after the hearing until April 21, 2025. (Tr. 63; AE C) Applicant provided two post-hearing exhibits, which were admitted into evidence without objection. (AE B; AE C)

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.1, 1.a.2, 1.a.3, 1.a.5, 1.a.7, and 1.a.9 with clarifications, extenuating, and mitigating information. (HE 3) She denied the allegations in SOR ¶¶ 1.a.4, 1.a.6, 1.a.8, 2.a, and 3.a with comments.

Applicant is a 70-year-old program manager who has been employed by a government contractor for 46 and ½ years. (Tr. 6, 8, 30) In 1972, she graduated from high school. (Tr. 6) In 1979, she received a bachelor's degree in mechanical engineering. (Tr. 7) She has not received any post-graduate education. (Tr. 7) In 1979, she married, and in 1985, she was divorced. (Tr. 7) She has lived with someone for 37 years. (Tr. 7) She does not have any children. (Tr. 8) She has never served in the military. (Tr. 8)

Personal conduct, handling protected information, and information technology systems

SOR ¶ 1.a alleges under the personal conduct guideline that Applicant's employer concluded that she was culpable for the following incidents:

1. In about 2017, Applicant allegedly failed to timely return Government Furnished Equipment (GFE), specifically two laptop computers, at the end of a contract despite multiple requests from the government customer. The laptops were ultimately retrieved from her in about July 2017 after the government security officer advised her employer's facility security officer (FSO) that legal action would be taken against her if the laptops were not returned.

The Navy issued two computers to Applicant's employer for her company to use on a technical-service contract (A). (Tr. 31, 33-35; GE 2 at 10; GE 3) She wanted to get the two computers transferred to technical-service contract (B), which had the same objective and customer as technical-service contract A. (Tr. 32-39; GE 2 at 7, 10) After technical-service contract A ended, the Navy wanted the two computers returned to the Navy. (GE 3) She retained the two computers for three months after technical-service contract A was concluded. (Tr. 36) She did not want to return the computers because they would need to be reprogramed and the data transferred when they were reissued. (Tr. 34, 39; GE 4) The contracting officer representative (COR) of technical-service contact A wanted her to return the computers. (GE 3) She coordinated with the COR of the new contract about retention of the two computers. (Tr. 39) She believed as program manager, she had authority to retain the two computers. (Tr. 36) The COR of technical-service contact A said he asked Applicant to return the computers on an unspecified date. (GE 3)

Applicant did not advise her supervisor that she was retaining the two computers. (Tr. 36) She did not receive a request to return the computers from the COR for technical service contract A until the end of the three months. (Tr. 38) She could not immediately return the computers upon request because she was in a meeting when the call was received about the computers. (Tr. 37) She advised the caller that she would return the two computers as soon as she could. (Tr. 37) On July 26, 2017, a government security official and her FSO went to Applicant's location and retrieved the two computers from her. (Tr. 37; GE 3; GE 4; GE 7) The Navy and security officials decided that there was no security violation, and no disciplinary action was taken against Applicant. (GE 2 at 7; GE 3; GE 4)

2. In about March 2019, Applicant allegedly failed to protect third-party information when she used her personal cell phone to discuss government business rather than a company-issued cell phone, in violation of company policy and the contract's DD Form 254.

Applicant had a company-issued phone for her use. (Tr. 42) She gave her personal telephone number to several colleagues and business-related friends. (Tr. 41-42) They discussed some business matters with her over her personal phone; however, nothing sensitive was discussed. (Tr. 41; GE 2 at 7) Applicant said her employer's policy was to use her business phone for employer-related conversations to the maximum extent possible. (Tr. 42) She was unaware of a policy precluding the use of a personal phone to conduct employer-related or government business. (Tr. 42) She believed the business phone was primarily issued to enable use of email from remote locations. (Tr. 42) She did not remember a specific prohibition against use of a personal phone to conduct business. (Tr. 43) A copy of the company policy concerning use of company-issued or personal cell phones was not included in the record. She noted that "a good portion of the general government and contractor population was using personal cell phones to conduct business in the new work from home environment." (HE 3 at 1) If there was a prohibition against use of personal cell phones to conduct contractor business, then a large number of violations would be occurring. (HE 3 at 1) She did not receive any disciplinary action as a result of this allegation. (GE 2 at 7)

3. In about December 2019, Applicant failed to properly secure the facility outer door when closing the facility for the evening after propping open the outer door to access the smoking area. In her April 19, 2023 Office of Personnel Management (OPM) interview, Applicant said that she propped the door open while she was outside smoking. (GE 2 at 6) When she reentered the facility, she closed the door. *Id*. The next day, her former manager gave her a warning about failing to ensure the door was secured. *Id*. She conceded at her hearing that she did not pull hard enough to completely close the door. (Tr. 43)

4. In about March 2020, Applicant allegedly failed to protect third-party information and failed to protect and properly mark documents and stored media after Navy security found sensitive documents and electronic media traced to her in an office she previously occupied.

Applicant denied the allegation in SOR ¶ 1.a.4. (Tr. 44) She said that she was not involved with classified documents, sensitive, or proprietary documents. (Tr. 45-46) In May 2017, she changed offices. (Tr. 44; GE 2 at 7) She was never shown what was found in the office she previously occupied. (Tr. 44) She said:

> [When I moved,] I had a minimum of three people ensure everything that was in my office or in my spaces had been cleared. Two years later, I was informed that there was some artifact that no one ever produced for me to be able to see that they claimed was in my office. Over the two-year time span between my exiting and the artifact surfacing, there had been two other people in that office, some of whom worked on programs that are parallel to what I was working on. And in some cases, there were actually artifacts that would transition from contractor to contractor or the government personnel that were also in that building. (Tr. 44) *See also* GE 2 at 7 (stating same).

Applicant did not receive any disciplinary action based on the allegation that sensitive information was found in the office she left in 2017. (GE 2 at 7)

5. In about December 2020, Applicant allegedly failed to properly secure GFE, namely a laptop, by keeping it at her home and not in an approved container for about fifteen months.

A coworker gave Applicant his Navy-issued computer because he needed it to be securely stored while they were changing offices. (Tr. 47; GE 2 at 6, 10) She put the computer into a banker's safe. (Tr. 47) She did not have the password to the computer. (GE 2 at 6) Her coworker lacked an access card for the computer. (GE 2 at 10) She retained this computer at her residence for about 10 months because she was the project manager, and the computer was related to a specific contract. (Tr. 46-48) Also, she was worried that it might be misplaced during the move. (GE 2 at 6) The computer was stored in compliance with telework procedures. (Tr. 48) She believed as the project manager she had authority to store the computer in her safe. (Tr. 49) She said she received emails about procedures to follow during COVID which supported her decisions. (Tr. 49) She

said she did not receive any disciplinary action for her possession or storage of the computer. (GE 2 at 6)

6. In about March 2022, Applicant's FSO allegedly questioned her about the location of the laptop she removed in December 2020 as discussed in 1.a.5, *supra*, and she stated that it had been returned in 2021. However, in about March 2022 she provided a DD Form 1149 receipt stating the laptop was returned on March 23, 2022. When questioned as to her statement to her FSO about returning the computer in 2021, she stated the laptop was stored in her home office until March 2022.

Applicant said when computers were moved out of the workplace for telework during COVID, they were not transferred on a DD Form 1149. (Tr. 51) In 2021, Applicant returned one or two laptops from her home; however, they did not include the laptop discussed in 5, *supra*. (Tr. 52) The laptops returned in 2021 were listed on a DD Form 1149. (Tr. 52)

Applicant documented the return of a laptop computer to the Navy in 2022 on a DD Form 1149. (Tr. 53; AE A at 15-17) The DD Form 1149 has the computer's serial number on the form. (AE A at 17) The DD Form 1149 indicates the date was changed from March 24, 2022, to March 23, 2022, which is consistent with the date by the signature of the person that received the computer. (AE A at 17) Applicant said the FSO was confused about which laptops were returned. (Tr. 50) The serial numbers were included on the DD Form 1149s. (Tr. 50) She provided the DD Form 1149s to the investigator. (Tr. 53) Applicant denied that she lied to the FSO when he asked about the computer in 2021. (GE 2 at 10) On March 27, 2022, she said that all laptops from a specific Navy source were returned in 2021. (AE A at 18)

On March 24, 2022, the FSO emailed Applicant that the contractor did not have records concerning two laptop computers, and he asked Applicant about laptops from a specific Navy source. (AE A at 19) Applicant provided a DD Form 1149 indicating on February 25, 2021, four computers were delivered to the Navy. (AE A at 20) The serial numbers of the four computers do not match the computer Applicant provided to the Navy on March 23, 2022.

In sum, Applicant and the FSO were discussing different computers. The FSO confused the computers returned to the Navy in 2021 and 2022. All computers were returned to the Navy.

7. In about mid-2021, Applicant was observed on a security camera removing boxes from the facility and placing them in her car. In about February 2022, she allegedly failed to promptly return documents as directed by her manager and FSO, including company contract information, government sensitive documents, and International Traffic in Arms Regulations (ITAR) information. On about March 24, 2022, she allegedly provided discrepant information in response to her FSO's inquiry about the whereabouts of the documents referenced above. She advised the FSO that she only had a few documents and personal affects at her home, however, on March 25, 2022, she was observed unloading approximately six large tubs from her vehicle. On about April 7, 2022, her FSO

inspected her office and observed that the tubs contained both company and government documents.

Applicant retained some of her employer's documents at home because she was working at home on a part-time basis during 2020 to 2021 during the COVID pandemic. (Tr. 55-56) She worked almost exclusively from home from January 2021 to October 2021 because of COVID. (GE 2 at 10) In January 2021, her employer moved out of the office to a new office. *Id*.

On February 22, 2022, Applicant's FSO sent an email advising contractor employees, including Applicant, to ensure sensitive and government CUI documents being used in home offices are protected from unauthorized individuals. (AE A at 9-10)

Applicant said she loaded documents into her vehicle, and the documents were a mixture of personal and employer's property. (Tr. 53-54; GE 2 at 6) The materials she loaded included vendor sheets. (Tr. 54) The vendor sheets were used to evaluate parts and vendor data. (Tr. 54) She denied that the vendor sheets were proprietary data. (Tr. 54) She put the materials in her vehicle because her office was being transferred to another location. (GE 2 at 6) In March 2022, her employer asked her to return the documents she placed into her vehicle. (Tr. 55) In March 2022, she brought six large tubs of documents from her home to her office. (Tr. 56) Some of the documents related to "preparing bids, doing forecasts, doing acquisitions, et cetera. So it was project related materials. Some of it was copies of emails, et cetera." (Tr. 56) She believed she was authorized to keep these documents at home so long as they were protected. (Tr. 56)

On March 29, 2022, Applicant's FSO sent her an email in which he told her to return "all government" and company documents to the contractor's facility not later than April 8, 2022. (AE A at 8) On March 30, 2022, Applicant's supervisor sent Applicant an email and CC'd her FSO indicating he "apologized for the turmoil this has caused [Applicant] and your customer." *Id.* Her manager said the issue was closed. (AE A at 8, 11)

Applicant's FSO said he issued a memorandum in April 2022 in which he said Applicant's manager and FSO indicated "government sensitive documents and International Traffic in Arms Regulations (ITAR) information" were supposed to be transferred from home offices to company offices. (GE 7 at 1) Applicant admitted to the FSO that the boxes she provided contained some company documents; however, she did not indicate they contained government sensitive documents or ITAR information. (GE 7 at 1) She did not receive any disciplinary action based on the allegations in SOR ¶ 1.a.7. (GE 2 at 6)

8. In a report dated April 5, 2022, Applicant's FSO alleged that Applicant made repeated false statements and impeded investigations and inquiries by directing government and her employer's employees to refrain from responding to the FSO.

The FSO's 1 ½ page letter listed most of the SOR allegations; however, he only described one incident in which he believed Applicant provided false information. He said

in December 2020 Applicant did not provide accurate information about when her coworker's computer was returned to the Navy. *See* SOR ¶¶ 1.a.5 and 1.a.6, *supra*. (GE 7) The FSO said Applicant told him the laptop computer was returned in 2021, and she returned the computer in 2022. (GE 5; GE 7) The FSO indicated that security had repeatedly referred Applicant to management for disciplinary action; however, management had not taken any adverse action against Applicant. (GE 7)

Applicant denied that she lied to the FSO. (Tr. 57) She acknowledged that she had difficulty communicating with the FSO because he was somewhat aggressive. (Tr. 57) She advised other employees that if they had difficulty answering the FSO's questions, they could direct the FSO to seek the information from her, and as the project manager, she could address his concerns. (Tr. 57) She denied that she told them not to cooperate with the FSO. (Tr. 57-58) She admitted that she was protective of her projects and customers. (GE 2 at 10)

9. In about October 2023, Applicant failed to properly secure the facility door when exiting the facility. Applicant closed the door upon leaving the facility, and she believed she heard it click, indicating it was locked. (Tr. 58) However, she conceded she may have been distracted, and she might not have fully closed and locked the door. (Tr. 58) She was aware that the door needed to be carefully checked because there were previous issues with locking properly. (GE 2 at 10) She received verbal counseling for this incident. *Id*.

On March 27, 2022, Applicant sent an email to management and the FSO in which she indicated the FSO had "inflamed the situation and mudd[ied[the waters," exceeded the scope of his authority, acted without an understanding of the government contract, and "added no value" to the process. (AE A at 3) She forwarded an email from the customer pertaining to security issues. (AE A at 4-7) The FSO then issued the 1 ½ page letter complaining about Applicant cited in SOR ¶ 1.a.8, *supra*. Applicant said the FSO may have been biased against her because of her email about the FSO's mishandling of a customer's access to facilities and computers. (GE 2 at 7-8) It is noteworthy that the FSO referred Applicant on April 6, 2022, to counterintelligence as a "possible Insider Threat." (GE 7 at 2)

Three coworkers provided statements describing the FSO as aggressive, unprofessional, hostile towards Applicant, and biased. (AE C at 16-18) One coworker indicated the contractor no longer employed the FSO who made a statement against Applicant. (AE C at 18)

Applicant's notes from an April 15, 2022, discussion with her FSO described the tone of the conversation as "unprofessional, disrespectful, intimidating, hos[tile], and threatening." (AE A at 22) She accused him of making misleading statements and disclosing to other employees that she was under a security investigation. *Id*. She described him as engaging in a "personal vendetta" against her. (AE A at 22)

SOR ¶ 2.a cross alleges under the handling protected information guideline, the information in subparagraphs 1.a.2, 1.a.3, 1.a.4, 1.a.7, and 1.a.9, above from the personal conduct guideline.

SOR ¶ 3.a cross alleges under the information technology systems guideline the information in subparagraphs 1.a.1, 1.a.4, and 1.a.5, above from the personal conduct guideline.

Character Evidence

Customers lauded Applicant and her team's work. (AE A at 24-30) She received an achievement award from her employer for her support to the Navy. (AE A at 32) The award description provides detailed praise of her outstanding contributions to the Navy. (AE A at 32) She has excellent performance evaluations from 2017 through 2022. (AE A at 33-90) Two coworkers described Applicant as competent, professional, honest, and trustworthy. (AE C at 14-15) She made numerous important contributions to her employer and customers. (AE B) Applicant has not received any adverse employee disciplinary actions. (Tr. 30) None of the SOR issues were documented in her performance reviews. (HE 3 at 4) She received two verbal warnings for failure to ensure doors were properly secured. *Id*.

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

Personal Conduct, Handling Protected Information, and Use of Information Technology

AG ¶ 15 describes the personal conduct security concern:

> 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 ¶ 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 ¶ 16 lists personal conduct disqualifying conditions that are potentially relevant in this case:

> (b) deliberately providing false or misleading information; or concealing or omitting information, concerning relevant facts to an employer, investigator, security official, competent medical or mental health professional involved in making a recommendation relevant to a national security eligibility determination, or other official government representative;
>
> (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.

AG ¶ 34 describes the handling protected information disqualifying conditions that are potentially relevant 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.

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.

SOR ¶ 2.a cross alleges under the handling protected information guideline, the information in subparagraphs 1.a.2, 1.a.3, 1.a.4, 1.a.7, and 1.a.9, from the personal conduct guideline. SOR ¶ 3.a cross alleges under the information technology systems guideline the information in subparagraphs 1.a.1, 1.a.4, and 1.a.5, from the personal conduct guideline.

SOR ¶ 1.a.1 alleges in about 2017, Applicant failed to timely return two Navy laptop computers when technical-service contract A ended. Applicant explained that as project manager she wanted to retain the two computers until data could be transferred to enable or facilitate the new Navy contract. Evidently, the Navy personnel responsible for accountability for the laptop computers were unaware of the necessity for transfer of the data. Eventually the Navy received the two computers. Applicant was responsible for the Navy contracts, and her temporary retention of two laptop computers until the Navy provided replacements was reasonable under the circumstances. There was no evidence that the Navy would have refused to permit her to retain the two laptop computers if her rationale was provided to the Navy. The information related to SOR ¶ 1.a.1 does not establish any disqualifying condition under the personal conduct or information technology guidelines.

SOR ¶ 1.a.2 alleges in about March 2019, Applicant failed to protect third party information when she used her personal cell phone to discuss government business rather than a company-issued cell phone, in violation of company policy and the contract's DD Form 254. An FSO who was biased against Applicant made this allegation. The company policy or DD Form 254 are not part of the record. Applicant said she did not discuss classified or sensitive information on her personal phone. DD Form 254s are used for classified information, and it is unclear why a DD Form 254 would address non-sensitive unclassified information. The information related to SOR ¶ 1.a.2 does not establish any disqualifying condition under the personal conduct or handling protected information guidelines.

SOR ¶ 1.a.3 alleges in about December 2019, Applicant failed to properly secure the facility outer door when closing the contractor's facility for the evening. SOR ¶ 1.a.9 alleges in about October 2023, Applicant failed to properly secure the contractor's facility door when exiting the facility. She was counseled after the first infraction. These two allegations are established. Applicant negligently failed to secure the door of the facility where she is employed on two occasions. The personal conduct and handling protected information disqualifying conditions in AG ¶¶ 16(d), 16(e), 34(g), and 34(h) are substantiated.

SOR ¶ 1.a.4 alleges in about March 2020, Applicant failed to protect third-party information and failed to protect and properly mark documents and stored media after Navy security found sensitive documents and electronic media traced to her in an office she previously occupied. Applicant left the office in 2017, and she said other employees inspected the office when she left to ensure nothing was left behind. Other employees working on the same contracts occupied the office after she left. She was never shown the documents the FSO said were traced to her. The FSO's allegation that the documents or stored media were traced to Applicant is not established by substantial evidence.

SOR ¶ 1.a.6 alleges Applicant lied to her FSO about turning in a computer in 2021. The contractor returned four computers to the Navy in 2021. Her FSO did not have visibility of the specific computer that Applicant retained at her residence. Applicant credibly stated that the FSO was mistaken about which computer she was referring to being returned to the Navy in 2021. She provided the requested computer on March 23, 2022, to the Navy. The FSO's allegation that Applicant lied is refuted.

SOR ¶ 1.a.7 alleges in about mid-2021, Applicant was observed on a security camera removing boxes from the contractor's facility and placing them in her car. In about February 2022, she allegedly failed to promptly return documents as directed by her manager and FSO, including company contract information, government sensitive documents, and International Traffic in Arms Regulations (ITAR) information. Applicant was authorized to remove from her contractor-provided office and store unclassified company documents in her residence because she was working at home. As to returning the documents after the FSO asked that they be returned, she did so within a reasonable period of time. Emails from management about the return of documents did not express any criticism of the timeliness of her return of the documents. The FSO's allegation of Applicant's wrongdoing is not established by substantial evidence.

SOR ¶ 1.a.8 alleges that, Applicant made repeated false statements and impeded investigations and inquiries by directing government and her employer's employees to refrain from responding to the FSO. The only false statement her FSO cited was the statement in SOR ¶ 1.a.6, which was refuted. There are no specific instances cited in which employees declined to answer questions based on Applicant's advice. She did not impede the investigation when she told her subordinates that they could tell the FSO to ask Applicant questions if they were uncomfortable responding to the FSO. A copy of the investigative report is not part of the record. The FSO's allegation in SOR ¶ 1.a.8 is refuted.

Personal conduct security concerns are refuted, except as indicated in the next paragraph. As indicated previously, personal conduct and handling protected information disqualifying conditions are substantiated with respect to Applicant's failure to ensure doors to the facility were locked on two occasions, and mitigating conditions under those guidelines must be considered. No disqualifying conditions for the use of information technology guideline are substantiated. Additional discussion is in the mitigation section, *infra*.

AG ¶ 17 lists conditions that could mitigate personal conduct security concerns:

> (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; and
>
> (e) the individual has taken positive steps to reduce or eliminate vulnerability to exploitation, manipulation, or duress.

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.

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 failed to properly secure the door of the contractor's facility in about December 2019 and October 2023. These are serious security infractions because someone could more easily enter the contractor's facility for nefarious purposes. Security officials and her supervisors are aware of these violations of security protocols, and she is not vulnerable to exploitation, manipulation, or duress by a foreign intelligence entity or other individual or group.

The mitigating conditions in AG ¶¶ 17(a) and 35(a) are established. The security violations were negligent and not intentional. The violations were infrequent (occurred twice) over a lengthy period of time. She has been sensitized to the importance of security and ensuring the doors are locked. I do not believe the failure to ensure doors are securely closed will recur. Her failure to secure the doors does not cast doubt on her current reliability, trustworthiness, and judgment. Personal conduct and handling protected information security concerns are mitigated.

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 E, K, and M 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 70-year-old program manager who has been employed by a government contractor for 46 and ½ years. In 1979, she received a bachelor's degree in mechanical engineering.

Customers lauded Applicant and her team's work. She received an achievement award from her employer for her support to the Navy. The award description provides detailed praise of her outstanding contributions to the Navy. She has excellent performance evaluations from 2017 through 2022. Two coworkers described Applicant as competent, honest, and trustworthy. She made numerous important contributions to her employer and customers.

I found Applicant to be a credible witness who is sincerely concerned about security issues and ensuring the success of the government contractor and making contributions to the Navy. The FSO is somewhat unreliable. He did not make allegations against Applicant until after she complained about his treatment of customers. Even if security concerns were not mitigated under the adjudicative guidelines, they would be mitigated under the whole-person concept.

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. Guidelines E (personal conduct), K (handling protected information), and M (information technology systems) security concerns are 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 E:	FOR APPLICANT
Subparagraphs 1.a.1 through 1.a.9:	For Applicant
Paragraph 2, Guideline K:	FOR APPLICANT
Subparagraph 2.a:	For Applicant
Paragraph 3, Guideline M:	FOR APPLICANT
Subparagraph 3.a:	For Applicant

Conclusion

Considering all of the circumstances presented by the record in this case, it is 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 granted.

_____
Mark Harvey
Administrative Judge