In the matter of:	)	
	)	
	)	ISCR Case No. 25-01230
	)	
Applicant for Security Clearance	)	
	)	

Appearances

For Government:
Troy L. Nussbaum, Esq., Department Counsel

For Applicant:
Ryan C. Nerney, Esq.

08/28/2026

Decision

GLENDON, John Bayard, Administrative Judge:

Applicant has not mitigated the security concerns under Guideline K (Handling Protected Information), Guideline M (Use of Protected Information), and Guideline E (Personal Conduct) arising from his actions. Applicant's eligibility for access to classified information is denied.

Statement of the Case

On November 25, 2025, the Defense Counterintelligence and Security Agency (DCSA) issued a Statement of Reasons (SOR) to Applicant detailing security concerns under Guidelines K, M, and E. The action was taken under Executive Order 10865, *Safeguarding Classified Information Within Industry* (February 20, 1960), as amended; Department of Defense (DOD) Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (January 2, 1992), as amended (Directive); and the adjudicative guidelines (AG) effective within DOD after June 8, 2017.

On March 3, 2026, Applicant responded to the SOR allegations through his attorney (Answer) and requested a hearing before an administrative judge from the Defense Office of Hearings and Appeals (DOHA). Department Counsel was prepared to proceed on May 18, 2026. The case was assigned to me the next day. On June 25, 2026, DOHA scheduled the case to be heard via Microsoft Teams video teleconference on July 16, 2026.

I convened the hearing as scheduled. Department Counsel offered seven documents marked as Government Exhibits (GE) 1 through 7 and presented the testimony of one witness. Applicant testified, and his attorney submitted nine documents marked as Applicant Exhibits (AE) A through I. At the request of Applicant's counsel, I left the record open until July 31, 2026, to give him the opportunity to submit additional documents. He timely provided seven proposed exhibits marked as AE J through AE P. All exhibits were admitted without objection. DOHA received the transcript of the hearing (Tr.) on July 23, 2026. (Tr. at 11-16, 253-254.)

Findings of Fact

Applicant is 49 years old. He married in 1994 and divorced in 2009. He remarried in 2010. He had one child with his first wife in 1994, and his second wife has two adult children from a prior marriage. He enlisted in the Air Force in 1994. He earned a bachelor's degree in 2018 and is presently studying for a master's. He received an honorable discharge from active duty in November 2000. He continued in the Air Force Reserve for more than a year. He began working in a series of five jobs with the U.S. Government until April 2025, for a total of over 30 years of Government service. His most recent government position was with the U.S. Military (Military) as a civilian tech manager. He was put on administrative leave in February 2022 and remained in that status until April 2025, at which time his federal employment was terminated. He presently works as a manager for a commercial business. He received his first security clearance in 1994. He is seeking to regain Top Secret and Sensitive Compartmented Information (TS/SCI) clearances at this time. His most recent Questionnaire for National Security Positions is dated April 1, 2021. (Tr. at 90-91, 95; GE 1 at 7, 11-15, 17, 20-22, 24-27, 34-37; GE 7; AE C; AE J at 2.)

The Government alleged in the SOR that Applicant is ineligible for national security eligibility because he mishandled the inventory of classified equipment, failed to account for and track protected equipment, and failed to protect classified information. The Government also alleged that his lax security practices resulted in the failure to account for protected equipment, and he provided false or misleading information in both a security interview and a memorandum for record. I find the following facts developed at the hearing and detailed in the documentary record:

Paragraph 1, Guideline K (Handling Sensitive Information)

SOR ¶ 1.a. 2019 - Inventory. In September 2019, Applicant began working as a civilian at a military site (the Site). He overlapped with his predecessor for about two months before the predecessor departed on terminal leave. At the beginning of his employment, Applicant was tasked with conducting a "turnover," annual inventory of all classified and sensitive equipment at the Site for which he was responsible. This required a verified, sighted confirmation of each device and a recordation of its location so that all the devices were accounted for before the turnover to Applicant was complete. He signed the inventory in November 2019 even though he had not completed it. (Tr. at 81, 99-106,108; GE 2 at 3-7; GE 5 at 7.)

After conducting the 2020 inventory the following year, Applicant reported on November 17, 2020, that three classified devices listed on his 2019 inventory were missing and should not have been included in Applicant's 2019 Inventory. In a Security Access Eligibility Report (SAER), dated December 11, 2020, (SAER I), a Site manager notified DCSA, which at that time operated under the name DOD Consolidated Adjudications Facility (DOD CAF), about this security incident. The report stated that Applicant confirmed that although he signed the 2019 inventory sheet, he had not completed the inventory. SAER I stated that two of the three missing classified devices were eventually found, but they were in an area that was not secured. These devices should have been in an approved safe for classified materials. Applicant and a senior IT security manager with authority over multiple sites (the Manager) both testified that no one ever found the third missing device. Applicant prepared a memorandum for record, dated December 13, 2020, in which he wrote that he "never laid hands or eyes on the items in question." He claimed that due to time constraints, "I did not step through the [draft] inventory [prepared by my predecessor] one by one with [my predecessor] like I should have." That memorandum was included in SAER I. (Tr. at 81, 99-106,108; GE 2 at 3-7; GE 5 at 7.)

The Manager testified that he reviewed the investigation into Applicant's flawed 2019 inventory and found the investigation to be thorough and its conclusions to be accurate. He noted that the errors in Applicant's inventory were serious because the largest risk of an inaccurate inventory was the potential compromise of classified information. The possibility of the loss of a classified device that was not properly inventoried raised that risk. One of Applicant's excuses for not sighting every piece of equipment as required for a complete inventory was that it would be necessary to take IT systems temporarily out of service so that the components could be taken apart and their serial numbers recorded. The Manager confirmed this point but maintained that the organization could continue to operate overall as individual systems were properly inventoried. The witness testified, "You have to make the time to conduct your inventories." He concluded that a proper inventory was more important than a temporary disruption of the operation of a system. (Tr. at 17-27.)

Applicant testified that in 2019 he requested to power down the systems to conduct the inventory and he was denied. Another problem he claimed he faced trying to conduct the inventory was that during his first month on the job, he was sent to a foreign country

to review certain matters there. Significantly, he further claimed that even though he could not physically conduct the inventory, he was pressured by two officials to sign the inventory. The officials were interviewed and denied Applicant's claims. Despite the circumstances, he signed the incomplete inventory as accurate. (Tr. at 101-110, 155; GE 5 at 7.)

The "Head" of the Site did not accept Applicant's excuses and issued a Letter of Reprimand, dated February 17, 2021, to Applicant. In the letter, the Head wrote, "Not only did you certify that all materials were accounted for when you had not verified their location, you also allowed this uncertainty to continue for another year." He then stated a critical, aggravating fact, "neglect handling of classified information could cause damage or irreparable injury to the United States." Applicant testified that he did not attempt to contest the Letter of Reprimand by filing a grievance. He said he was too busy. (Tr. at 155-157, 224-225; GE 3 at 1; GE 5 at 7-8.)

A follow-up SAER, dated February 28, 2021, (SAER II) forwarded a command investigation letter, dated January 11, 2021, that reviewed the incident described above. SAER II states that Applicant had not acted in a "nefarious way, nor did he attempt to hide the issue when discovered." The report set forth procedures to avoid a repeat of this incident whenever there is a "turnover in a position similar to this." SAER II recommended that Applicant's SCI accesses and eligibility "remain." The DOD CAF favorably adjudicated this security incident in late 2022. In a SAER, dated April 17, 2023, (SAER III) setting forth information that was subsequently developed and is described below under the heading SOR ¶ 1.d, the Commanding Officer requested reconsideration of this adjudication. (Tr. at 81-82; GE 4 at 10-11; GE 5 at 6.)

SOR ¶ 1.b. 2021 - Failure to Inventory and Account for Four Laptops. In January 2021, Applicant learned that four new laptops were received at the Site and were plugged into classified ports for configuration, which made them classified devices. He only visually confirmed three of the four laptops. He did not attempt to track down the fourth laptop, and he did not ensure that all of the laptops were properly configured and entered into the inventory. He also made no attempt to confirm that the laptops were being tracked. A subsequent inventory in July 2021 revealed that the four classified laptops were missing. After the Command conducted exhaustive searches, three of the four laptops were located. (GE 5 at 8-9, 27-28.)

On September 28, 2021, the Manager commenced a preliminary inquiry into these events. Applicant left work early that day after claiming he received an emergency call from his wife. He testified that she had been diagnosed with cancer. The next morning, Applicant arrived at his office and claimed that he found the missing laptop, a fifth laptop, which was unclassified, and an unclassified tablet. He reported that he found the three devices on a chair in the back of his office covered by his sweater, which he always left in his office. The fourth laptop had been missing since March 4, 2021. The other two devices were not previously known to be missing. Applicant claimed he did not know how the devices appeared in his office after they were not discovered during exhaustive

searches of the Site. (Tr. at 27-39, 58-65, 85-89, 108-119, 157-165, 181; GE 4 at 4-5; GE 5 at 10, 28-32, 35, 38.)

SEAR III reported that Applicant's explanations for a number of related events surrounding his discovery of the three devices lacked candor. One claim he made was that he was not the custodian of the devices and had not used them. A February 2022 forensic analysis of the three items discovered Applicant's digital fingerprints on the tablet. The analysis revealed that Applicant had used the tablet on multiple occasions and contained his credentials for his personal email, other personal accounts, and his driver's license number. Applicant denied any knowledge of the tablet. The Manager also concluded that the circumstances surrounding the appearance of the missing fourth classified laptop, the unclassified laptop, and the tablet were suspicious, and Applicant had not been candid in denying any knowledge of the three devices. (Tr. at 27-39, 58-65, 85-89, 108-119, 157-165, 181; GE 4 at 4-5; GE 5 at 10, 28-32, 35, 38.)

Applicant submitted a memorandum for record, dated February 24, 2022, in response to the investigation of the three devices. He noted that he had used a Military tablet during personal travel and that this tablet was not listed on his inventory of all tablets at the Site. Applicant's explanations were not accepted by management, and he was debriefed from access to the Military program on February 27, 2022. His local access to TS/SCI information was also suspended. (GE 5 at 10; AE B.)

During the investigation, Applicant provided a complicated explanation of what happened with the original four classified laptops that went missing. He said that it was not his job to inventory and account for these laptops. He argued that the laptops were intended for a different organization and to be used offsite. He also said that the security official of that part of the organization never communicated with him about the arrival of the laptops. However, he admitted in a memorandum for record, dated October 14, 2021, that he had become aware of the four laptops in January 2021. As the IT Manager, it was his responsibility to configure the laptops. (Tr. at 67-68, 86, 108-119, 173-198; GE 4 at 4-5; GE 5 at 21-30, 33-38; AE K and AE L.)

At the time of the investigation and at the hearing, Applicant said that he believed someone put the fourth laptop on his office chair. The Manager did not accept any of Applicant's explanations and excuses as valid or truthful. He determined that it was in the best interest of national security to debrief Applicant from program access. After Applicant was interviewed about the tablet with his information, he was escorted out of the facility and put on administrative leave. Senior management at the Site also decided to debrief Applicant from accessing SCI and recommended that Applicant's SCI eligibility be suspended. (Tr. at 67-68, 86, 108-119, 173-198; GE 4 at 4-5; GE 5 at 21-30, 33-38; AE K and AE L.)

SOR ¶ 1.c. 2022 - Discovery of Applicant's Failure to Secure Sensitive Equipment. In February 2022, it was discovered that three sensitive communication devices were missing. The devices were used at that time for classified communications.

Applicant served as the tech manager at the Site, had the collateral role of the manager for communication security, and was ultimately responsible for securing the devices and the related encryption components. He charged the security guards with the responsibility of checking for the devices at the end of every day. It was reported in the April 2023 SAER III that two devices were found in a drawer in an IT office and the third device was found under papers on Applicant's desk. The Manager was not certain that each device found was accompanied with its encryption component. Proper security procedures required that the encryption component be removed, and the component be locked in an approved safe. (Tr. at 40-45, 65-66, 71-74, 86-88, 119-125, 198-205; GE 5 at 10, 47.)

Part of Applicant's security role was to inventory and track these devices and the encryption components. The investigation of the missing devices determined that Applicant could not show the encryption components were accounted for nor could he explain why they were not accounted for. He testified that none of the encryption components were in the devices when they were found. He said the encryption components were supposed to be with the individuals to whom they were issued or in their personal safes. Shortly after this incident, Applicant was put on administrative leave and a second Letter of Reprimand was issued. The issue of the missing encryption components was not resolved before he was debriefed. He testified, however, that he was subsequently advised that all three encryption components were located. (Tr. at 40-45, 65-66, 71-74, 86-88, 119-125, 198-205, 225; GE 5 at 10, 47.)

At the hearing, Applicant explained that the three devices were assigned to very senior officials at the Site. At the time the devices were discovered as missing, the offices of the officials were being renovated, and the officials were not at the Site. He speculated that the devices were probably handed to someone on his IT staff and put in a storage area. He was never advised that they had been removed from their normal locations in the offices of the officials. He did not explain how one device ended up on his desk. (Tr. at 204-205, 225.)

SOR ¶ 1.d. 2023 - Discovery of Classified Documents in an Unauthorized Storage Container. In February 2022, Applicant was debriefed and escorted off the Site. About a year later, 100 or so SCI classified documents were discovered in his former office in locked drawers in a cabinet that was not accredited to store classified information. Unclassified documents were also found in the cabinet co-mingled with the classified documents. Applicant's former office was being renovated for the next occupant. During the renovation, the locked cabinet was drilled open because no one had the key to the cabinet. The Manager testified that he assumed Applicant's office had been occupied in the year after he was removed from the premises, but he was not sure. In SAER III, it was concluded that "the cabinet drawers in question have not been accessed since [Applicant] stopped working at the [Site] approximately one year ago." Many of the documents carried Applicant's name, evidencing that they were in fact his documents. Applicant's actions violated DOD rules regarding the storage of SCI documents. This was treated as a fourth security incident by Applicant in a two-year period. (Tr. at 45-48, 75-79, 125-134, 206-208; GE 5 at 6 to 50, 52.)

At the hearing, Applicant testified that he did nothing wrong. He denied that he kept classified documents in a locked cabinet, and he even denied that there was any such cabinet in his office at the time he was placed on administrative leave. He testified that he had a box of classified and unclassified documents on his desk when he was called to be interviewed and then escorted off the Site. He said that someone occupied his former office after he was debriefed. He speculated that someone must have introduced the cabinet into his former office and stored the documents in the cabinet without leaving a key, even though the classified documents were required to be stored in an approved safe. He also claimed that when he was debriefed, he turned over all of the keys, so that if there was a cabinet in his office at that time, management had the key for the cabinet. He believes that the contents of his box of documents is what was found. He asserted that there was nothing wrong with his actions of having this box of classified documents unsecured in his office during the working day (Tr. at 45-48, 75-79, 125-134, 206-213, 228, 238; GE 5 at 6 at 50-52; AE D.)

SOR ¶ 1.e. Lax Security Practices Continued Despite Prior Letter of Reprimand. The Government contends that the four security incidents involving Applicant described above constituted a pattern of lax security practices. This behavior continued even though a Letter of Reprimand was issued in February 2021 after the 2019 inventory security incident. In a Command Recommendation, the senior officer at the Site wrote, "I have lost all trust and confidence in this employee [Applicant], and he cannot be relied upon to properly safeguard classified information at any level, especially the critical and special sensitive information." (Tr. at 239-240; GE 5 at 15.)

Paragraph 2, Guideline M (Use of Information Technology)

SOR ¶ 2.a. February 2022 Discovery of Sensitive Communication Equipment Despite Prior Letter of Reprimand. See discussion in SOR ¶ 1.c, above.

Paragraph 3, Guideline E (Personal Conduct)

SOR ¶ 3.a. Issuance of Letter of Reprimand. As noted above, the Head of the Site issued a Letter of Reprimand to Applicant on February 17, 2021, criticizing his "lack of care in verifying the classified inventory," referring to his mishandling of the 2019 inventory. As noted above, Applicant presented multiple excuses for his actions. They were all rejected by management. Significantly, Applicant never took full responsibility for his mistake in signing the inventory without doing the necessary work.

SOR ¶ 3.b. Falsification during Security Interview. Applicant was interviewed on January 13, 2022, about the missing classified laptop and the two other devices he claimed he "found" in his office in September 2021. He stated during the interview that he had not known the locations of the devices prior to their discovery and that he was not the owner or custodian of the devices. As noted above, a forensic analysis of one of the devices, the tablet, contained evidence that he had accessed the device on multiple occasions for personal use. Applicant's interview statement was false. After the forensic

analysis was competed, Applicant was interviewed again, and he repeated his claim that he knew nothing about the tablet. When confronted with the results of the forensic analysis, Applicant continued to deny any knowledge about the tablet or how it appeared in his office. At the hearing, Applicant provided a different and confusing timeline and denied that he was questioned in the January 13, 2022 interview about being the owner or custodian of any of the devices he found in his office. Therefore, he testified that he did not provide any false information about the devices. SAER II directly contradicts that testimony. Again, Applicant has not admitted or accepted any responsibility for providing any misinformation during the security interview. (Tr. at 137-142; GE 4 at 4; GE 5 at 31-38.)

SOR ¶ 3.c. Omission of material Information in January 2022 Memorandum for the Record. As noted above, Applicant claimed that he "found" the missing fourth classified laptop and the two other devices on a chair in his office. On January 28, 2022, he prepared a memorandum for record regarding the three devices. He failed to discuss in that memorandum that he possessed and accessed the tablet as discussed in sections above discussing SOR ¶¶ 1.b and 3.b. At the hearing, Applicant explained his omission on the basis that he had no idea that the particular tablet he had used for personal purposes while on travel was the same tablet that he found in the chair of his office. He asserted that he did not intentionally mislead anyone by his comments in the memorandum for record. Management concluded that under all of the circumstances developed in its inquiry, Applicant must have known that he had used the tablet in question for personal purposes and that his statement was untrue. Applicant has never accepted responsibility for his actions with respect to the tablet and his omission of material information in the January 28, 2022 memorandum. (Tr. at 142-144; GE 5 at 30-38; AE N at 3.)

Character and Mitigating Evidence

Applicant's counsel submitted an extensive set of exhibits and supplemental exhibits. I have carefully reviewed the four character letters submitted with the Answer, his reviews for his last two years in his position at the Site, awards he received, and a Certificate of Completion of a behavior modification course taken by Applicant in 2026. (AE D; AE E; AE F; AE H.)

I have also carefully reviewed Applicant's seven supplemental exhibits that were submitted after the hearing. These exhibits included a statement of reasons issued by DCSA that preceded the SOR. Applicant's response to that earlier statement of reasons is also included. In addition, Applicant submitted four exhibits that consisted of multipage documents and multiple documents addressing the issues discussed above. (AE K; AE L; AE M; AE N; AE O; AE P.)

Policies

When evaluating an applicant's suitability for national security eligibility, the administrative judge must consider the adjudicative guidelines. In addition to brief introductory explanations for each guideline, the adjudicative guidelines (AG list potentially disqualifying conditions and mitigating conditions, which are to be used in evaluating an applicant's national security eligibility.

These guidelines are not inflexible rules of law. Instead, recognizing the complexities of human behavior, these guidelines are applied in conjunction with the factors listed in AG ¶ 2 describing the adjudicative process. The administrative judge's overarching adjudicative goal is a fair, impartial, and commonsense decision. The entire process is a conscientious scrutiny of applicable guidelines in the context of a number of variables known as the whole-person concept. The administrative judge must consider all available, reliable information about the person, past and present, favorable and unfavorable, in making a decision.

The protection of the national security is the paramount consideration. AG ¶ 2(b) requires, "Any doubt concerning personnel being considered for national security eligibility will be resolved in favor of the national security." In reaching this decision, I have drawn only those conclusions that are reasonable, logical, and based on the evidence contained in the record. I have not drawn inferences based on mere speculation or conjecture.

Directive ¶ E3.1.14, requires the Government to present evidence to establish controverted facts alleged in the SOR. Under Directive ¶ E3.1.15, "The applicant is responsible for presenting witnesses and other evidence to rebut, explain, extenuate, or mitigate facts admitted by the applicant or proven by Department Counsel, and has the ultimate burden of persuasion as to obtaining a favorable clearance decision."

A person who seeks access to classified information enters into a fiduciary relationship with the Government predicated upon trust and confidence. This relationship transcends normal duty hours and endures throughout off-duty hours. The Government reposes a high degree of trust and confidence in individuals to whom it grants national security eligibility. Decisions include, by necessity, consideration of the possible risk the applicant may deliberately or inadvertently fail to protect or safeguard classified information. Such decisions entail a certain degree of legally permissible extrapolation as to potential, rather than actual, risk of compromise of classified or sensitive information. Finally, as emphasized in Section 7 of Executive Order 10865, "Any determination under this order adverse to an applicant shall be a determination in terms of the national interest and shall in no sense be a determination as to the loyalty of the applicant concerned." *See also* Executive Order 12968, Section 3.1(b) (listing multiple prerequisites for access to classified or sensitive information.)

Analysis

Paragraph 1, Guideline K (Handling Protected Information)

The security concerns relating to the guideline for handling protected information concerns are set out in AG ¶ 33, which reads in pertinent part:

> 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 sets forth two disqualifying conditions that have possible application to the facts of this case:

> (g) any failure to comply with rules for the protection of classified or sensitive information; and
>
> (h) negligence or lax security practices that persist despite counseling by management.

The record evidence established AG ¶¶ 34(g) and 34(h) with respect to the SOR allegations in SOR ¶¶ 1(a), 1(b), 1(d), and 1(e). The Government's extensive evidence with respect to each of these allegations overwhelmingly supports those SOR allegations.

The evidence with respect to SOR ¶ 1(c) is different. It shows that the Military strongly believed that Applicant had mishandled the security of the three devices and encryption components. However, the evidence also established that the three senior individuals who were assigned to use the devices had retained the responsibility for securing them when they were away from their offices. They failed to take the necessary steps, and I cannot conclude that the evidence established that this responsibility was then passed over to Applicant. The allegation in SOR ¶ 1(e) is based upon the allegation in SOR ¶ 1(c), which I have ruled in favor of Applicant. Accordingly, I also find SOR ¶ 1(e) in Applicant's favor.

The burden, therefore, shifts to Applicant to mitigate the remaining security concerns under Guideline K. The guideline includes the following four conditions in AG ¶ 35 that can mitigate security concerns arising from handling protected information:

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

(b) the individual responded favorably to counseling or remedial security training and now demonstrates a positive attitude toward the discharge of security responsibilities;

(c) the security violations were due to improper or inadequate training or unclear instructions; and

(d) the violation was inadvertent, it was promptly reported, there is no evidence of compromise, and it does not suggest a pattern.

Applicant did not establish any of the above potentially mitigating conditions. He based his case on his denial of any wrongdoing in any of the security incidents. In light of the strength of the Government's documentary evidence against Applicant, his denials lacked credibility. He tried to blame his defective 2019 inventory on others and circumstances beyond his control. None of his excuses are supported by any documentary evidence or justified his actions. His story about finding three devices on his office chair after extensive searches of the Site did not locate them does not successfully point the responsibility for the sudden appearance of the devices at anyone but himself.

Applicant's claim that the cabinet in his former office in which the classified documents were found did not exist when he worked at the Site is equally implausible. His effort to shift responsibility for storing classified documents improperly to some unknown third party rests on a simple factual claim. He asserts that he had no such cabinet in that office at the time he was suspended, which requires the assumption that a later occupant brought the cabinet to the office and decided to store classified documents in it even though it was not an approved safe for such documents. Applicant's theory not only lacks corroborating evidence, it is also simply not credible that the next occupant of that office would not hand any unsecured classified documents found in a box in the office over to an appropriate security official. It makes no sense that the occupant would instead store the classified documents in a cabinet brought into the office rather than in an approved safe.

Paragraph 2, Guideline M (Use of Protected Information)

The security concerns relating to the guideline for the failure to comply with rules and procedures pertaining to information technology systems are set out in AG ¶ 39:

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 ¶ 40 sets forth one disqualifying condition that has possible application to the facts of this case:

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

The record evidence did not establish the above potentially disqualifying condition. Applicant was counseled in a February 2021 letter of reprimand that his actions were not acceptable. However, I have found the February 2022 incident alleged in SOR ¶ 1.c, above, in favor of Applicant. Accordingly, I conclude that the Government has not met its burden of establishing a security concern under Guideline M as alleged in the SOR.

Paragraph 3, Guideline E (Personal Conduct)

The security concerns relating to the guideline for personal conduct are set out in AG ¶ 15:

> Conduct involving questionable judgment, lack of candor, dishonesty, or unwillingness to comply with rules and regulations can raise questions about an individual's reliability, trustworthiness, and ability to protect classified or sensitive information.

AG ¶ 16 sets forth seven potentially disqualifying conditions that apply to the facts of 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; and
>
> (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.

The record evidence established that Applicant deliberately provided false or misleading information or omitted relevant facts to his employer, the investigator, and security officials during the investigations of the 2019 inventory and the missing classified devices. The investigation into the mishandled classified documents occurred after he had been removed from his security position. The record sets forth significant adverse information in multiple adjudicative areas that, when considered as a whole, supports a whole-person assessment of questionable judgment, untrustworthiness, unreliability, lack of candor, and unwillingness to comply with rules and regulations. His employer went so far as to issue a Letter of Reprimand for his actions with respect to the 2019 mishandled and incomplete inventory, but Applicant's lax security practices continued. Further, there is significant evidence that supports a whole-person assessment of questionable judgment, untrustworthiness, unreliability, lack of candor, and unwillingness to comply with rules and regulations. This evidence includes evidence of inappropriate behavior, a pattern of rule violations, providing false information, omitting material information in statements, and significant misuse of the Military's security and technology assets and his employer's time investigating matters of security concern.

The burden, therefore, shifts to Applicant to mitigate security concerns under Guideline E. The guideline includes the following two conditions in AG ¶ 17 that can mitigate security concerns arising from improper personal conduct:

> (a) the individual made prompt, good-faith efforts to correct the omission, concealment, or falsification before being confronted with the facts;
>
> (c) the offense is so minor, or so much time has passed, or the behavior is so infrequent, or it happened under such unique circumstances that it is unlikely to recur and does not cast doubt on the individual's reliability, trustworthiness, or good judgment; and

> (d) the individual has acknowledged the behavior and obtained counseling to change the behavior or taken other positive steps to alleviate the stressors, circumstances, or factors that contributed to untrustworthy, unreliable, or other inappropriate behavior, and such behavior is unlikely to recur.

Applicant has not established any of the above potentially mitigating conditions. He did not make a prompt good faith effort to correct his omission or concealment of facts. His offenses are not minor, and they were frequent enough so as to evidence a pattern of behavior. Also, the offenses cast doubt on his reliability, trustworthiness, and good judgment. Significantly, Applicant has not acknowledged his misconduct. The counseling he obtained in 2026 was merely a four-hour course in behavior modification and is nothing more than a token effort to show changed behavior. There is nothing in the record to suggest real change and that his behavior is unlikely to recur.

Whole-Person Concept

Under the whole-person concept, the administrative judge must evaluate an applicant's eligibility for national security eligibility by considering the totality of the applicant's conduct and all relevant circumstances. The administrative judge should consider the nine adjudicative process factors listed at AG ¶ 2(d):

> (1) the nature, extent, and seriousness of the conduct; (2) the circumstances surrounding the conduct, to include knowledgeable participation; (3) the frequency and recency of the conduct; (4) the individual's age and maturity at the time of the conduct; (5) the extent to which participation is voluntary; (6) the presence or absence of rehabilitation and other permanent behavioral changes; (7) the motivation for the conduct; (8) the potential for pressure, coercion, exploitation, or duress; and (9) the likelihood of continuation or recurrence.

Under AG ¶ 2(c), the ultimate determination of whether to grant national security eligibility for a security clearance must be an overall commonsense judgment based upon careful consideration of the guidelines and the whole-person concept. I considered the above whole-person factors and the potentially disqualifying and mitigating conditions in each of the adjudicative guidelines in light of all pertinent facts and circumstances surrounding this case. I have given weight to the comments made by Applicant's character references and to his military service and many years of government employment. Applicant's failure to accept responsibility and his unpersuasive effort to pass the blame to others for the security problems he created undercut the mitigating value of the evidence he has produced in rebuttal to the Government's case. Overall, the record evidence leaves me with questions and doubts as to Applicant's present suitability for national security eligibility and a security clearance.

Formal Findings

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

Paragraph 1, Guideline K:	AGAINST APPLICANT
Subparagraphs 1.a and 1.b:	Against Applicant
Subparagraph 1.c:	For Applicant
Subparagraphs 1.d and 1.e:	Against Applicant
Paragraph 2, Guideline M:	FOR APPLICANT
Subparagraph 2.a:	For Applicant
Paragraph 3, Guideline E:	AGAINST APPLICANT
Subparagraphs 3a. through 3.c:	Against Applicant

Conclusion

In light of all of the circumstances presented by the record in this case, I conclude that it is not clearly consistent with the interests of national security to grant Applicant's eligibility for a security clearance. Eligibility for access to classified information is denied.

John Bayard Glendon
Administrative Judge