DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 19-02174
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Mary Margaret Foreman, Esq., Department Counsel
For Applicant: *Pro se*

11/22/2021

_____

Decision

_____

CERVI, Gregg A., Administrative Judge

This case involves security concerns raised under Guideline K (Handling Protected Information) and Guideline E (Personal Conduct). Eligibility for access to classified information is denied.

Statement of the Case

Applicant submitted a security clearance application (SCA) on August 3, 2018, 2020. On October 16, 2020, the Department of Defense Consolidated Adjudications Facility (now known as the Defense Counterintelligence and Security Agency Consolidated Adjudications Facility (DCSA CAF) sent him a Statement of Reasons (SOR) alleging security concerns under Guidelines K and E. The DCSA CAF acted under Executive Order (Exec. Or.) 10865, *Safeguarding Classified Information within Industry* (February 20, 1960), as amended; DOD Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (January 2, 1992), as amended (Directive); and the adjudicative guidelines (AG) effective June 8, 2017.

Applicant answered the SOR on February 4, 2021 (Ans.), and requested a decision based on the written record without a hearing. The Government's written brief with

supporting documents, known as the file of relevant material (FORM), was submitted by Department Counsel on May 26, 2021. A complete copy of the FORM was provided to Applicant, who was afforded an opportunity to file objections and submit material to refute, rebut, or mitigate the security concerns. Applicant received the FORM on June 26, 2021, but did not submit a reply or object to any evidence submitted with the FORM. The case was assigned to me on September 8, 2021. Government Exhibits (GE) 1 through 8 are admitted into evidence without objection.

Findings of Fact

Applicant is a 67-year-old employee of a defense contractor, employed since 2018. He served in the U.S. Army Reserve from 1989 to 2002, and on active duty in the U.S. Army from 2002 to 2015, when he retired. He received an honorable discharge and retired at the rank of Chief Warrant Officer 3. He also served in a foreign country military from 1969 to 1987, before he became a naturalized U.S. citizen. He reported attending college at two universities, but not receiving a degree. He married in 1982 and has two adult children. He does not currently hold a security clearance.

The SOR alleges under Guideline K that in June 2015, while serving on active duty in the U.S. Army, Applicant received a general officer memorandum of reprimand (GOMR) for improperly transporting and storing classified information and for possessing six government computers at his residence, both in violation of the Uniform Code of Military Justice (UCMJ); and that his local access was suspended in about October 2014. (SOR ¶ 1.a) The SOR also alleges that Applicant was unable to account for a classified government external hard drive, and that when he was requested to return the hard drive, he substituted a different drive that contained another agency marking and the remnants of a "secret" sticker. Applicant was unable to explain how he gained possession of the agency hard drive. (SOR ¶ 1.b)

Under Guideline E, Applicant is alleged to have falsified his 2018 SCA by disclosing his reprimand and claiming that it was for "slack observation of security policy," when in fact it was a reprimand for negligence and failure to maintain the standards expected of a U.S. Army Officer and [agency] technician after over 4,000 documents and imagery files classified as SECRET, TOP SECRET/SCI, or otherwise classified/protected were found on government computers and other media stored in his private residence, as described in SOR ¶ 1.a. (SOR ¶ 2.a) The SOR also alleges Applicant falsified his 2018 SCA by deliberately failing to disclose that his security eligibility/access authorization was suspended in about October 2014. (SOR ¶ 2.b)

Finally, the SOR alleges that Applicant concealed and misrepresented material facts during the course of his personal subject interview, conducted by a government security investigator in October 2018 and February 2019, by stating that the reprimand for "slack observation of security policy" listed in his SCA, concerned taking a personal cell phone into a sensitive compartmented information facility (SCIF) where he was working, and that "there were no adverse finding from the searches" of his property. In truth, the SOR contends that Applicant received a GOMR after over 4,000 documents

and imagery files classified as SECRET, TOP SECRET/SCI, or otherwise classified/protected, and six government computers, were discovered in his personal residence as described in SOR ¶ 1.a. The investigation into these matters was terminated in December 2015 after Applicant refused to cooperate with U.S. Army Intelligence (USAI) investigators. (SOR ¶ 2.c) Applicant answered the SOR by "admitting" certain facts with explanations; however, he did not admit the SOR allegations as presented. (Ans.) Therefore, I will consider Applicant's answer as a general denial of the SOR allegations but with explanatory testimonial evidence.

In June 2013, Applicant's unit conducted an "AR 15-6" investigation into allegations of potential security violations against Applicant. The investigation concluded that Applicant committed security violations under Army regulations. Applicant worked in a SCIF and had access to classified documents and data. In November 2012, a systems and hardware inventory was conducted in the SCIF where Applicant worked, and discovered that an external hard drive that "may have once been under the control" of Applicant was not accounted for. Applicant had been seen plugging a similar hard drive into his classified (SIPR) computer days prior to the inspection. A coworker also saw Applicant use a hard drive marked "unclassified" that he retrieved from his personal backpack and insert it into a classified computer. Applicant's coworkers suspected that the hard drive was the same drive missing from the SCIF, as they often saw the hard drive plugged into Applicant's computer during the day, but sometimes missing at night. (Item 6)

In November 2012, a 100% entry and exit inspection was conducted inside the SCIF. When Applicant approached the inspection area and observed workers emptying out their pockets for inspection, Applicant dropped his backpack off at the inspection site and abruptly headed back toward his work area. When he returned to retrieve his backpack, it was searched, and a stack of loose CDs were found. Some were marked SECRET/NOFORN. Applicant explained that he was taking the CDs to another office, but he was instructed that classified CDs could not be transported inside a personal backpack and that he needed a proper container for such purposes. After permitting Applicant to take the CDs to the office, it was later discovered that he never left them at the office as he claimed.

An inspection of the SCIF also found Applicant's cell phone in his desk drawer, which is prohibited inside a SCIF. Upon questioning, Applicant admitted to having an unauthorized cell phone in the SCIF, improperly transporting classified media in his personal belongings, uploading an unclassified hard drive into a classified system, and uploading an improperly labeled CD in a classified system.

Applicant denied having any knowledge of the missing hard drive, but claimed another hard drive with a classified sticker that he was using in the SCIF was "scrubbed" and he took it home. He was asked to retrieve the hard drive from his home. He returned with a hard drive with the classified sticker scratched off but with another sticker in it showing it was from a government agency. The investigator determined that this was not the same hard drive that was missing from the SCIF. (Item 6)

Applicant consented to a search of his home. In his garage, investigators found six Government desktop computers and monitors, and 13 black cases containing agency CDs. Applicant had arranged for the computer equipment to be shipped to another location, but his possession of the equipment at his residence was not authorized. Some of the equipment contained files marked as limited distribution, including NATO Unclassified, NATO Restricted, and NATO SECRET. Applicant's personal media devices contained a large number of highly classified documents with markings as high as TOP SECRET/NOFORN. In all, Applicant possessed over 4,000 documents and imagery files classified up to TOP SECRET/SCI and 86 archived files which contained material marked SECRET on government and personal computers and media storage devices at his residence. Applicant admitted bringing a personal, unauthorized cell phone into the SCIF, improper handling and safeguarding classified and protected information, personally declassifying media devices without proper authority, and intentionally taking and transporting classified media to his personal residence.

Although investigators did not find evidence that Applicant transferred information to an unauthorized individual or entity, foreign or otherwise, he did connect his government computers to the internet at various times and he had a Skype contact list with 17 entries for users in foreign countries. Over 20 USB and external storage devices had been connected to Applicant's laptop at some time, many of which were not included in the original seizure. Applicant generally denied to Army investigators any wrongdoing or intentional possession of classified information. He voluntarily permitted initial inspection, but denied permission for an enhanced inspection of his devices by a specialized cyber counterintelligence office. Investigators obtained a command search authorization instead. (Items 6 and 7) According to Applicant's JPAS incident history, his local access was suspended during the investigation on or about October 2014, and remained suspended. Applicant's commander recommended his security clearance be revoked on or about October 2015. (Item 5)

On June 19, 2015, Applicant received a General Officer Memorandum of Reprimand (GOMR) from his commanding general. He was reprimanded for improperly transporting and storing classified information, possessing six government computers at his residence, in violation of the UCMJ. He was reprimanded for his negligence and for failure to maintain the standards expect of him as an Army officer and technician holding a TS/SCI clearance. (Item 8) He acknowledged receipt of the reprimand on July 14, 2015 without submitting any rebuttal matters within the time period allotted. The GOMR was filed in his official Army personnel record. (Item 8)

Applicant completed his SCA on August 3, 2018. In section 13A – Employment Activities, he listed his active duty employment history. In response to a question about whether he received any discipline or warnings, he noted that he received an "official reprimand" in July 2015, and listed the reason as "slack observation of security policy." In his answers to questions on his 2018 SCA, section 25 – Investigations and Clearance Record – Denied Clearance, asking whether he ever had a "security clearance eligibility/access authorization denied, suspended, or revoked," he stated "no," and failed to disclose his suspended access authorization.

Applicant was interviewed by a government security investigator on October 17, 2018 and February 25, 2019. He certified the resulting personal subject interview summary as accurate on August 23, 2019. He discussed his official reprimand for "slack observation of security policy" and claimed the issue occurred when he left his personal cell phone in the SCIF where he worked. He was aware of the security violation and acknowledged that he made a mistake and was forgetful. He stated that his technology devices were inspected as a result, but there were "no adverse findings from the searches." (Item 4) He noted that he was given a verbal and written reprimand for slack observation of security policy, issued by an unrecalled "major." He stated that he was not disciplined or suspended for the incident, and that he has not misused any information technology system, to include failing to complying with rules, procedures, guidelines or regulations that may raise a security concern about his reliability, trustworthiness, or willingness to protect such systems. (Item 4)

In Applicant's answer to the SOR on February 4, 2021, he noted in response to the Guideline K SOR allegation ¶ 1.a, that he was issued a GOMR rather than judicial action because "mitigating circumstances prevailed." He claimed that the government computers found at his home were legitimately transferred from an agency school to Army units. He claimed that the computers were at his residence because they were wiped clean and he needed to connect to the internet for updates. In response to SOR ¶ 1.b, he claimed that the classified hard drive missing from the SCIF was used by all soldiers assigned to the unit, but he accepted responsibility as the ranking officer. He stated that he allowed inspection of all hard drives in his possession to "verify my personal innocence."

In his response to Guideline E, SOR allegation ¶ 2.a, Applicant stated that he admitted to the government security investigator that he was reprimanded, and referred the investigator to his official records as he felt constrained to discuss it in a "public setting." In response to SOR ¶ 2.b, he stated that he transferred out of a classified setting in November 2012 and worked until he retired in December 2015 and that "all I was aware of was that I was read-off and did not need to know." In response to SOR ¶ 1.c (regarding his statement during his summary interview), he noted that he was "referring to an incident with a cell phone not to the circumstances that caused a General Officer reprimand. That investigation was concluded with the reprimand and I officially retired from the U.S. Army in December 2015." (Ans.)

Law and Policies

"[N]o 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 applicants 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 § 2.

National security eligibility 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, an administrative judge applies these guidelines 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 a person's stability, trustworthiness, reliability, discretion, character, honesty, and judgment. AG ¶ 1(b).

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 that 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 made "in terms of the national interest and shall in no sense be a determination as to the loyalty of the applicant concerned." Exec. Or. 10865 § 7. Thus, a decision to deny a security clearance is merely an indication the applicant has not met the strict guidelines the President and the Secretary of Defense 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. *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, e.g.,* ISCR Case No. 12-01295 at 3 (App. Bd. Jan. 20, 2015).

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 burden of proving a mitigating condition, and the burden of disproving it never shifts to the Government. *See, e.g.,* ISCR Case No. 02-31154 at 5 (App. Bd. Sep. 22, 2005).

An applicant "has the ultimate burden of demonstrating that it is clearly consistent with the national interest to grant or continue his security clearance." ISCR Case No. 01-20700 at 3 (App. Bd. Dec. 19, 2002). "[S]ecurity clearance determinations should err, if they must, on the side of denials." *Egan*, 484 U.S. at 531; *see,* AG ¶ 1(d).

Analysis

Guideline K: Handling Protected Information

AG ¶ 33 expresses 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.

Relevant conditions that could raise a security concern under AG ¶ 34 and may be disqualifying include:

> (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;
>
> (e) copying or modifying protected information in an unauthorized manner designed to conceal or remove classification or other document control markings; and
>
> (g) any failure to comply with rules for the protection of classified or sensitive information.

Applicant's security violations are sufficient to implicate disqualifying security concerns under AG ¶¶ 34 (b), (c), (e), and (g).

Relevant conditions that could mitigate security concerns under AG ¶ 35 include:

> (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.

While Applicant was on active duty working with highly sensitive material, he showed an intentional disregard for security procedures and regulations, both while working in a SCIF and in taking government equipment and substantial amounts of classified information to his home. He received a GOMR from an Army general officer, and was suspended from local access. Applicant's wrongful conduct in 2012 and 2013, while working with substantial classified information, was of such a nature as to cast serious doubt on his reliability, trustworthiness, and good judgment. His recent efforts to minimize or obscure his past questionable conduct while reapplying for a security clearance compound the doubts about his current reliability, trustworthiness, and good judgment. Based on the record, I am not convinced that Applicant fully appreciates the seriousness of his past questionable conduct, and therefore I am not convinced that similar conduct will not continue.

Applicant's intentional conduct with respect to protection of classified material and pattern of security violations is indicative of a problem with security awareness and a persistent lapse of expected conduct while working within a classified environment. Applicant's SCA, personal subject interview, and Answer to the SOR did little to diminish my concerns. The pattern of violations and subsequent effort to obfuscate the investigation findings and GOMR language leads me to question Applicant's future behavior with respect to security awareness and following rules and regulations for the safe handling of classified information. No mitigation is appropriate.

Guideline E: Personal Conduct

AG ¶ 15 expresses 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 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 describes conditions that could raise a security concern and may be disqualifying in this case. The following disqualifying condition are potentially applicable:

> (a) deliberate omission, concealment, or falsification of relevant facts from any personnel security questionnaire, personal history statement, or similar form used to conduct investigations, determine employment qualifications, award benefits or status, determine national security eligibility or trustworthiness, or award fiduciary responsibilities; and

(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.

The record is sufficient to implicate disqualifying conditions under AG ¶¶ 16(a) and (b). Applicant's response to SCA question 13A showed an effort to minimize the gravity of his past conduct while reporting receipt of an official reprimand. While "slack observation of security policy" may be interpreted broadly to include Applicant's conduct, I find that this language intentionally minimizes and obscures the conduct for which he was reprimanded. I also find that he intentionally failed to report his suspended access in response to SCA section 25. Finally, I find that he intentionally concealed and misrepresented material facts regarding the breath of his past security violations when describing the reason for his reprimand while being interviewed by a government security investigator.

Guideline E includes conditions that could mitigate security concerns arising from personal conduct. I have considered all of the mitigating conditions under AG ¶ 17 and found the following relevant:

(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; and

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

Applicant's incomplete and obtuse answers to questions in his SCA, his subject interview, and his failure to report his access suspension in his SCA, shows a continued effort to minimize or obscure his conduct and raises serious questions about his current

truthfulness and candor. He has failed to provide information sufficient to implicate the mitigating conditions under Guideline E.

Whole-Person Concept

Under AG ¶¶ 2(a), 2(c), and 2(d), the ultimate determination of whether to grant national security eligibility must be an overall commonsense judgment based upon careful consideration of the guidelines and the whole-person concept. Under the whole-person concept, the administrative judge must evaluate an applicant's eligibility for a security clearance by considering the totality of the applicant's conduct and all relevant circumstances. The administrative judge should consider the nine adjudicative process factors listed at AG ¶ 2(d). Although adverse information concerning a single criterion may not be sufficient for an unfavorable eligibility determination, the individual may be found ineligible if available information reflects a recent or recurring pattern of questionable judgment, irresponsibility, or unstable behavior. AG ¶ 2(e).

I considered all of the potentially disqualifying and mitigating conditions in light of the facts and circumstances surrounding this case. I have incorporated my findings of fact and comments under Guidelines K and E in my whole-person analysis. Applicant was an officer with experience and clearances necessary for properly handling classified information in sensitive spaces. The pattern of security violations is indicative of a persistent problem that has not been shown to be rectified, and his intentional misrepresentation on the SCA and during his subject interview cement my concerns about his reliability and trustworthiness. The record evidence and consideration of the whole-person adjudicative factors are not sufficient to overcome the handling protected information and personal conduct concerns raised in the SOR.

Overall, the record evidence leaves me with questions and doubts as to Applicant's eligibility for access to classified information.

Formal Findings

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

Paragraph 1, Guideline K:	AGAINST APPLICANT
Subparagraphs 1.a and 1.b:	Against Applicant
Paragraph 2, Guideline E:	AGAINST APPLICANT
Subparagraphs 2.a – 2.c:	Against Applicant

Conclusion

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

_____
Gregg A. Cervi
Administrative Judge