DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
----------	)	ISCR Case No. 22-01687
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Aubrey De Angelis, Esq., Department Counsel
For Applicant: *Pro se*

04/24/2023

_____

Decision

_____

WESLEY, ROGER C. Administrative Judge

Based upon a review of the case file, pleadings, exhibits, and testimony, Applicant did not mitigate handling protected information and use of information technology concerns. Eligibility for access to classified information or to hold a sensitive position is denied.

Statement of the Case

On September 12, 2022, the Defense Counterintelligence and Security Agency (DCSA) Consolidated Adjudications Facility (CAF) issued a statement of reasons (SOR) to Applicant detailing reasons why under the handling protected information and use of information technology guidelines the DCSA CAF could not make the preliminary affirmative determination of eligibility for granting a security clearance, and recommended referral to an administrative judge to determine whether a security clearance should be granted, continued, denied, or revoked. The action was taken under Executive Order (Exec. Or.) 10865, *Safeguarding Classified Information within Industry* (February 20, 1960); Department of Defense (DoD) Directive 5220.6 *Defense Industrial Personnel Security Clearance Review Program,* (January 2, 1992) (Directive); 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.

Applicant responded to the SOR (undated), and elected to have his case decided on the basis of the written record, in lieu of a hearing. Applicant received the File of Relevant Material (FORM) on January 31, 2023, and interposed no objections to the materials in the FORM. He did not respond to the FORM, and the case was assigned to me on April 11, 2023.

Summary of Pleadings

Under Guideline K, Applicant allegedly committed multiple security infractions that were followed by verbal and written warnings between October 2019 and March 2021. Allegedly, these infractions and warnings are of continuing security concern. The allegations are cross-alleged under Guideline M.

In Applicant's response to the SOR, he admitted all but one of the allegations with explanations. He denied only the allegations of SOR ¶ 1.b, allowing access and use of unauthorized software (Skype). He claimed there was no classified information involved in his cited October 2019 downloading infraction. He also claimed that the hard drive he failed to properly secure in 2020 and 2021 he inherited from the person who previously occupied his cubicle.

Applicant claimed generally there was no formal process in place to perform a complete inventory of his office cubicle office when he started his employment with his current employer. And, he claimed he has proven his trustworthiness through his work as a system administrator, in which he handled thousands of classified hard drives and system tapes, performed hundreds of software installations, and ensured that the classified systems he was responsible for were compliant with all DoD security requirements for the previous five plus years.

Findings of Fact

Applicant is a 60-year-old civilian of a defense contractor who seeks a security clearance. Allegations covered in the SOR and admitted by Applicant are incorporated and adopted as relevant and material findings. Additional findings follow.

Background

Applicant married in June 2003 and has six children (ages 17, 15, 14, 12, 9, and 8) from this marriage. (Item 4) Applicant earned a bachelors degree in December 1997 and a master's degree in May 2006. (Item 4) He enlisted in the Marine Corps in January 1980 and served six years in the Inactive Reserve before receiving an honorable discharge in June 1986. (Item 4)

Since March 2016, Applicant has worked for his current employer as a computer systems technologist. (Item 4) Between November 2003 and March 2016, he worked for other employers in various systems administrator positions. (Item 4) He has held a security clearance since April 2004. (Item 4)

Applicant's security infractions

Between October 2019 and November 2020, Applicant received multiple verbal warnings for security infractions, and more recently, in March 2021, a written warning for failing to properly secure a classified hard drive while in a closed area. (Items 4-6) Records document that in October 2019, Applicant self-reported to his information security systems officer (ISSO) that he downloaded classified information on a compact disc (CD) without authorization in September 2019 and left it unsecured on his desk in his cubicle until October 2019. (Item 6)

Further investigation by his ISSO confirmed that Applicant had downloaded 12 files to a CD without authorization, failed to document the trusted downloads (TD) in e-Binder, and failed to properly label and secure the CD. His ISSO administrators found no loss or compromise of classified information and advised him of the need to properly download classified information in the future to ensure his understanding of proper downloading procedures. (Item 6)

In April 2020, Applicant (while employed by his current employer) received a security infraction notification with a verbal warning for allowing access and use of unauthorized software (Skype) on a classified information system without following required cybersecurity procedures. (Item 3) Applicant denied parts of the substantive allegation, claiming the software had been approved by his ISSO administrator. However, he admitted that his further testing of the software was unauthorized. (Item 3)

In their own investigation of the April 2020 incident, Applicant's ISSO administrators confirmed that another employee of the company was in the process of getting the Skype for business software certified for use on the company's information system (inclusive of ensuring that certain security controls were on the system and certified for use) when the employee discovered that Applicant had been allowing employees to use the program before the full certification could be finalized. (Item 6) While no loss or compromise of classified information was detected, Applicant was issued a verbal warning. (Item 6)

In May 2020, while still employed by his current employer, Applicant committed a company policy infraction when he inadvertently brought a cell phone into a closed area. (Items 3 and 6) Employer records affirm that Applicant self-reported the incident, and his employer's ISSO administrators confirmed the absence of any compromise of classified information.

Upon concluding their investigation, his ISSO administrators verbally warned him of his violation without the issuance of a security infraction. ISSO administrators, in turn, referred their findings to Applicant's supervisor for any further consideration of the incident. (Item 6) Company records confirmed that Applicant received a company policy infraction with corrective actions deferred to management for inadvertently bringing a cell phone into a closed area, in violation of established procedures. (Item 6)

Applicant's employment records document that in November 2020, he self-reported his failure to secure a classified hard drive while in a closed area. (Items 3 and 6) Admitting the infraction, Applicant told his company's ISSO administrator that he had found the classified hard drive in his desk drawer, but could not recall how the drive arrived in his cubical. (Item 6) He told the ISSO administrator investigating the incident that he last used similar drives in 2016 upon his new arrival to the company. (Item 6) ISSO administrators, in turn took possession of the hard drive and found no nefarious activities or anomalies in their audit. (Item 6)

ISSO administrators based their findings on the absence of any exhibited activity with the hard drive since 2016. (Item 6) Although, Applicant's actions were confirmed to be inadvertent, he was considered to be responsible for violating established safeguard procedures for storing materials bearing secret labels (as was the case with the hard drive found in his cubicle drawer), and was issued a verbal warning. Applicant's claims that there was no formal process to inventory their cubes when he first entered his employment with his employer were neither acknowledged nor accepted by ISSO administrators. (Items 3 and 6)

More recently (in March 2021), Applicant received a written warning for failing to properly secure a classified hard drive while in a closed area. (Items 3 and 6) Claiming he inherited the hard-drive from a person who occupied the cubicle before him, he acknowledged the incident and claimed he was told to accept the hard drive "as-is" when he assumed possession of the hard-drive as a new employee. (Item 3) Applicant's employer's records reflect that Applicant acquired his hard drive in 2018, and the drive was found when an employee of the company was moving into Applicant's cubical. (item 6) When asked by ISSO administrators about the hard drive, Applicant acknowledged his acquiring the drive when he joined the company in 2018 (believing at the time that the drive was unclassified).

ISSO administrators in their investigation of the 2021 incident found Applicant's acquired hard drive to bear a classified label (albeit in a clear case with an unclassified sticker on the exterior), and, as such, was a classified hard drive that was improperly stored by Applicant for approximately two years without any evidence of a suspected loss or compromise of classified information. (Item 6) Based on the investigation's findings, Applicant received a written warning.

Since the investigated March 2021 incident, Applicant has been transferred to a new position where he is no longer responsible for classified assets. (Item 5) He assured in his personal subject interview (PSI), conducted in February 2022, that should he be assigned to another position in the chain of assets, he will be sure to check the inventory and ensure that all items are properly labeled. (Item 5)

In his defense, Applicant expressed his belief that he had proved his trustworthiness through his work as a system administrator entrusted with the responsibility for handling "thousands of classified hard drives/tapes, performed hundreds software installations, and ensured the classified information systems that he was responsible for were compliant with DoD requirements for over 5 years." (Item 3)

Policies

By virtue of the jurisprudential principles recognized by the U.S. Supreme Court in *Department of the Navy v. Egan*, 484 U.S. 518, 528 (1988), "no one has a 'right' to a security clearance." 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. Eligibility for access to classified information may only be granted "upon a finding that it is clearly consistent with the national interest to do so." Exec. Or. 10865, *Safeguarding Classified Information within Industry* § 2 (Feb. 20, 1960), as amended.

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

The AGs list guidelines to be considered by judges in the decision-making process covering DOHA cases. These guidelines take into account factors that could create a potential conflict of interest for the individual applicant, as well as considerations that could affect the individual's reliability, trustworthiness, and ability to protect classified information. These guidelines include conditions that could raise a security concern and may be disqualifying (disqualifying conditions), if any, and all of the conditions that could mitigate security concerns, if any. These guidelines must be considered before deciding whether or not a security clearance should be granted, continued, or denied. Although, the guidelines do not require judges to place exclusive reliance on the enumerated disqualifying and mitigating conditions in the guidelines in arriving at a decision.

In addition to the relevant AGs, judges must take into account the pertinent considerations for assessing extenuation and mitigation set forth in ¶ 2(a) of the AGs, which are intended to assist the judges in reaching a fair and impartial, commonsense decision based on a careful consideration of the pertinent guidelines within the context of the whole person. The adjudicative process is designed to examine a sufficient period of an applicant's life to enable predictive judgments to be made about whether the applicant is an acceptable security risk.

When evaluating an applicant's conduct, the relevant guidelines are to be considered together with the following ¶ 2(d) factors: (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 of the conduct; (8) the potential for

pressure, coercion, exploitation, or duress; and (9) the likelihood of continuation or recurrence.

Viewing the issues raised and evidence as a whole, the following individual guidelines are pertinent herein:

Handling Protected Information

> *The 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 and individual's trustworthiness, judgment, reliability, or willingness and ability to safeguard such information, and is a serious security concern. . . . AG ¶ 33.

Use of Information Technology

> *The 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 ¶ 40.

Burdens of Proof

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. *See also* Exec. Or. 12968 (Aug. 2, 1995), § 3.1.

Initially, the Government must establish, by substantial evidence, conditions in the personal or professional history of the applicant that may disqualify the applicant from being eligible for access to classified information. The Government has the burden of establishing controverted facts alleged in the SOR. *See Egan*, 484 U.S. at 531. "Substantial evidence" is "more than a scintilla but less than a preponderance." *See v.*

Washington Metro. Area Transit Auth., 36 F.3d 375, 380 (4th Cir. 1994). The guidelines presume a nexus or rational connection between proven conduct under any of the criteria listed therein and an applicant's security suitability. *See* ISCR Case No. 95-0611 at 2 (App. Bd. May 2, 1996).

Once the Government establishes a disqualifying condition by substantial evidence, the burden shifts to the applicant to rebut, explain, extenuate, or mitigate the facts. Directive ¶ E3.1.15. An applicant "has the ultimate burden of demonstrating that it is clearly consistent with the national interest to grant or continue his [or her] security clearance." ISCR Case No. 01-20700 at 3 (App. Bd. Dec. 19, 2002). The burden of disproving a mitigating condition never shifts to the Government. *See* ISCR Case No. 02-31154 at 5 (App. Bd. Sep. 22, 2005). "[S]ecurity clearance determinations should err, if they must, on the side of denials." *Egan*, 484 U.S. at 531; *see* AG ¶ 2(b).

Analysis

Security concerns are raised over Applicant's documented history of multiple infractions of established procedures for protecting classified information over a three-year period (2019-2021) and ensuing warnings (both verbal and written). Although there is no probative evidence of loss or compromise of classified materials, security concerns remain over Applicant's history of unauthorized misuse of classified information systems that required warnings and demands for corrective actions by his employer's security and management personnel.

Applicant's repeated negligent infractions of classified systems owned and operated by his employer warrant the application of DCs covered by Guideline K: DC ¶¶ 34(g), "any failure to comply with rules for the protection of classified or sensitive information," and 34(h) "negligence or lax security habits that persist despite counseling by management"; apply to Applicant's situation. Applicable DCs under Guideline M are DCs ¶¶ 40(e), "unauthorized use of a government or other information technology system," and 40(g), "negligent or lax security habits in handling information technology that persist despite counseling by management," apply as well.

To be sure, none of the investigations prompted by Applicant's reported inadvertent misuse and mishandling of his employer's classified procedures and processes resulted in any loss or compromise of classified materials. Nonetheless, his multiple breaches of established classified procedures and processes over an extended period of time (despite prior warnings and instructions) pose serious trust and judgment issues that effect his eligibility to access sensitive or classified information, or hold a sensitive position of trust. For mitigation purposes herein, the passage of time since his last reported infraction in 2021 is still relatively recent.

In the face of proven acts of pattern negligence in misusing his employer's procedures and processes for accessing and protecting classified information, Applicant's acknowledgments of his judgment lapses and claims of learned lessons come too late to meet the mitigating requirements of any of the potentially available mitigating conditions under Guideline K as well as those covered by Guideline M.

Applicant's acknowledged breaches of established procedures and processes for accessing classified procedures and processes breaches are still too recent to facilitate safe predictions of recurrence avoidance in the foreseeable future.

While this is not a close case, even close cases must be resolved in the favor of the national security. *See Dept. of Navy v. Egan*, *supra*. Quite apart from any required adherence to rules and regulations the Government may impose on the clearance holder employed by a defense contractor, the Government has the right to expect care and good judgment from the trust relationship it has with the clearance holder. *See Snepp v. United States*, 444 U.S. 507, 511n.6 (1980)

Whole-person assessment

From a whole-person perspective, Applicant has failed to establish enough independent probative evidence of his overall trustworthiness, maturity, and good judgment required of those who seek eligibility to hold a security clearance or sensitive position. At this time, he lacks enough positive reinforcements and time in his demonstrated safe use of classified procedures and processes to facilitate safe predictions that he is at no risk of recurrence.

Considering the record as a whole at this time, and granting due weight to the acknowledgements made by Applicant of his past trust breaches and steps he is taking to avoid any recurrences, there is insufficient probative evidence of sustainable mitigation in the record to make safe predictable judgments about Applicant's ability to avert recurrent trust breaches in the future when tasked with responsibility for protecting sensitive and classified information. Taking into account all of the facts and circumstances surrounding Applicant's pattern misuse of classified procedures and processes over the course of several years of documented infractions involving classified information, he does not mitigate security concerns with respect to the allegations covered by SOR Guideline K, and M.

I have carefully applied the law, as set forth in *Department of Navy v. Egan,* 484 U.S. 518 (1988), Exec. Or. 10865, the Directive, and the AGs, to the facts and circumstances in the context of the whole person, I conclude handling protected information and use of information technology security concerns are not mitigated. Eligibility for access to classified information is denied.

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:

GUIDELINE K (HANDLING PROTECTED INFORMATION): AGAINST APPLICANT

Subparagraphs 1.a-1.e: Against Applicant

GUIDELINE M (USE OF INFORMATION TECHNOLOGY): AGAINST APPLICANT

Subparagraph 2.a: Against Applicant

Conclusion

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

_____
Roger C. Wesley
Administrative Judge