DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
----------	)	ISCR Case No. 21-00624
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Andrew Henderson, Esq., Department Counsel
For Applicant: Thomas E. Higgins, Esq.

02/07/2023

_____

Decision

_____

WESLEY, ROGER C. Administrative Judge

Based upon a review of the case file, pleadings, and exhibits, Applicant did not mitigate personal conduct, 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 29, 2021, the Defense Counterintelligence and Security Agency (DCSA) Consolidated Adjudications Facility (CAF) issued a statement of reasons (SOR) to Applicant detailing reasons why under the personal conduct, handling protected information, and use of information technology guidelines the DoD 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); *Defense Industrial Personnel Security Clearance Review Program,* DoD Directive 5220.6 (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 on November 18, 2021, and requested a hearing. The case was assigned to me on April 23, 2022. A hearing was scheduled for December 19, 2022, and heard on the date as scheduled. At the hearing, the Government's case consisted of three exhibits and two hearing exhibits (HEs I-II) that were admitted for administrative notice over Applicant's relevance objections. (GEs 1-3 and HEs I and II; Tr. 33). Applicant relied on one witness (herself) and no exhibits. The transcript (Tr.) was received on January 3, 2023.

Summary of Pleadings

Under Guideline E, Applicant allegedly was fired from her employment at a U.S. federal court in August 2019 for accessing court records that she did not have permission to access and is ineligible for rehire. These Guideline E allegations are cross-alleged under Guidelines K and M for allegedly (a) violating her employer's computer usage policy by intentionally receiving sealed documents filed with her court employer without authorization and (b) assessing sensitive documents outside of a business need to know approximately 28 times while employed as a courtroom deputy clerk for a federal court.

In Applicant's response to the SOR, Applicant admitted the allegations in the SOR with explanations and clarifications. She claimed that approximately 85 to 90% of federal criminal cases in her federal district court involved either illegal entry or alien smuggling. She also claimed that she accessed sealed files in the court out of curiosity over rarer cases in her court and never for personal gain or for the furtherance of an improper purpose. She further claimed that she never knew nor currently knows a single person named in any of the files and never transmitted, communicated, or sent to anyone, at any time, information included in the contents of the sealed files.

Findings of Fact

Applicant is a 48-year-old civilian of a defense contractor who seeks a security clearance. The admitted allegations are incorporated and adopted as relevant and material findings. Additional findings follow.

Background

Applicant never married and has three children from prior relationships, ages 24, 15, and 14. (GEs 1-2; Tr. 18) She earned a high school diploma in May 1993 and a bachelor's degree in 2005. (GE 1-2) She reported no military service.

Since October 2019, Applicant has been employed by her current defense contractor as an administrative assistant. (GEs 1-2; Tr. 13, 19) Between November 2007 and August 2019, she was employed as a deputy clerk of a federal court. (GEs 1-2; Tr. 14, 18) She reported unemployment between August 2019 and October 2019. (GEs 1-2) She has never held a security clearance. (GE 1)

Applicant's access to court files

In August 2019, Applicant was fired from her employment as a courtroom deputy for a federal district court for cited accessing sealed court files that she did not have permission to access. (GEs 1-3; Tr. 14, 19-20, 27)

Fully briefed and aware of her employer's computer usage policy, Applicant intentionally accessed sealed documents digitally filed with her court employer without authorization or need to know in or about July 2019. (GEs 1-3; Tr. 24-25) The court files she accessed were sensitive documents covering ongoing criminal proceedings involving a highly dangerous local drug, racketeering, and murderous gang. (HEs I-II) Applicant accessed these documents 28 times while employer as a courtroom deputy clerk with neither authorization nor a demonstrated need to know. (GEs 1-3) Whether she ever passed along information from the sealed files she accessed to unauthorized third persons remains unproven from the received evidence. Applicant for her part denied ever disclosing any of the contents of the sealed files she accessed to her friend of many years, and there is no evidence in the record to materially challenge and contradict her. (Tr. 14)

In an interview conducted by the court's executive court clerk and Applicant's overall supervisor in August 2019, Applicant was informed that she violated the court's computer usage policy, as well as Canon 2 of the Code of Conduct for Judicial Employees. (GE 3) During her meeting with the court's senior clerk, she and the court clerk discussed her accessing sealed documents filed with the court. (GE 3) Acknowledging that she accessed sealed documents involving a pending criminal case covering a certain criminal defendant associated with a notorious drug trafficking, murdering, and racketeering gang, she explained that she had done so "out of curiosity" because it was a big case in her community. (GE 3)

Asked by the interviewing senior court clerk about her access frequency, she replied that she could not recall. (GE 3) Questioned about whether she had ever printed, forwarded, or distributed information from the court files she accessed, she indicated that she had not. (GE 3; Tr. 14) Asked further whether she had any friends affiliated with the gang, she replied that she had an undisclosed friend who gave birth to a baby fathered by an identified member of the street gang. (GE 3; Tr. 28)

Upon further investigation of the records covering the sealed files access incident, the court's senior clerk and his office documented 28 separate incidents of Applicant's accessing the sealed files covering the pending cases without authorization or demonstrated need to know. (GE 3) Accessing sealed court files without authorization of demonstrated need to know constituted a direct violation of the court's computer usage policy. (GE 3) Applicant's awareness of the court's computer use policy is imputed to Applicant by virtue of her signing the court's computer use policy agreement acknowledging and confirming her responsibility to comply with the policy's requirements. (GE 3)

Asked in her interview with the senior court clerk whether she had viewed sealed information in other court cases more than five times without authorization or a need to know, she initially expressed uncertainty how many times she had done so before acknowledging multiple instances of unauthorized access. (GE 3; Tr. 20, 23, 26, and 30) Pressed further about her accessing court files in the pending street gang criminal case, Applicant told the court clerk that while she had heard of the local street gang referenced in the sealed files, she did not know any of the gang members. (GE 3)) Upon further questioning, she acknowledged having a friend who had a baby with one of the gang members. (GE 3)

Finding that Applicant had not been initially forthright about her friend's relationship with the gang member, the interviewing court clerk concluded that Applicant individually and collectively breached Canon 2 of the Code of Conduct for Judicial Employees and implicitly violated the trust and confidence placed in her by the court. (GE 3) Based on the clerk's careful consideration of the conditions and requirements of her position, he terminated her employment with the court. Applicant's separation did not include any reserved future eligibility for rehire consideration.

In her own hearing testimony, Applicant could not supply any more information on her relationship with her friend and the latter's links to the local street gang member. (Tr. 30) Nor could she shed any further light about what intentions she harbored when accessing the sealed files in issue beyond curiosity over a heavily reported case in the media. (Tr. 16-18, 30-32) Applicant was at all times fully aware of the serious security concerns posed by the street gang charged with murder, drug trafficking, and racketeering in the pending criminal proceeding in her community. (HE I) While she has not maintained any Facebook or other contact with any of the 19 indicted street gang members referenced in the sealed files she accessed, she still maintains a friendship with this friend who is linked to the local street gang member. (Tr. 28)

In her most recent personal subject interview (PSI) conducted in April 2020, Applicant expounded more on her breach of her court's computer use policy and ensuing separation from federal service. (GE 2) In her PSI, she volunteered that she was the only one involved in the sealed file incident and was not authorized to access the sealed court files.

She assured the investigating agent that she had no reason to access the court files other than her harboring curiosity about the highly publicized case. (GE 2) She further assured the investigator that she had learned her lesson and is now better informed of what she is allowed and not allowed to do. (GE 2) Applicant's curiosity assurances cannot be inferentially reconciled with her friendship with the friend in a parenting relationship with one of the gang members or with the number of times (28) she accessed the sealed files in issue.

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 AG 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. The AG 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:

Personal Conduct

The Concern: Conduct involving questionable judgment, lack of candor, dishonesty, or unwillingness to comply with rules and regulation can raise questions about an individual's reliability, and 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 ¶ 15.

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 firing from her federal deputy court position over her unauthorized accessing of sealed criminal records maintained in the federal court where she was employed for the past 12 years. While there is no cognitive evidence of disclosure of any of the information in the files, her unauthorized access violated both her court employer's computer usage policy and Canon 2 of the Code of Conduct for Judicial Employees.

Applicant's repeated unauthorized accessing of sealed court files (28 times in all) while employed as a deputy court clerk with no need to know the contents of the files she accessed warrant the application of DCs covered by Guideline K. DC ¶ 16(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 information," is applicable to Applicant's situation.

While there is no probative evidence of any third-party disclosure of the contents of the sealed files accessed by Applicant without authorization, her multiple breaches of her court's computer use policy and governing canons applicable to her employment position pose serious trust and judgment issues that impact her eligibility to access sensitive or classified information, or hold a sensitive position of trust. For mitigation purposes herein, the passage of time since her 2019 sealed files access incident (less than four years) is still relatively recent.

In the face of proven acts of repetitive unauthorized access to sensitive sealed criminal files during her employment as a deputy court clerk, Applicant's acknowledgments of her judgment lapses and claims of learned lessons come too late to meet the mitigating requirements of MC ¶ 17(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." More time is needed to reestablish the level of trust needed to hold a position of trust.

Cross-alleged under Guidelines K and M are Applicant's unauthorized accessing of sealed criminal files. Applicable DCs under Guideline K are DC ¶¶ 34(d), "inappropriate efforts to obtain or view protected information outside one's need to know"; 34 (f), "viewing or downloading information from a secure system when the information is beyond the individual's need to know"; and 34(g), "any failure to comply with rules for the protection of classified or sensitive information." Applicable DCs under Guideline M are DCs ¶¶ 40(c), "use of any information technology system to gain unauthorized access to another system or to a compartmented area within the same system," and "40(e), "unauthorized use of any information technology system."

With less than four years of elapsed time since Applicant's proven acts of unauthorized access to sealed criminal court files and ensuing termination from her employment, too little time has passed to credit Applicant with any of the potential mitigating conditions under any of the raised Guidelines. Applicant's 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 honesty 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 her overall honesty, trustworthiness, maturity and good judgment required of those who seek eligibility to hold a security clearance or sensitive position. At this time, she lacks enough positive reinforcements and time in a trust position to facilitate safe predictions of she 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 her past trust breaches and steps she 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 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 unauthorized access actions in the past with her federal court employer, she does not mitigate security concerns with respect to the allegations covered by SOR Guidelines E, 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 personal conduct, 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 E (PERSONAL CONDUCT):	AGAINST APPLICANT
Subparagraph 1a:	Against Applicant
GUIDELINE K (HANDLING PROTECTED INFORMATION):	AGAINST APPLICANT
Subparagraphs 2.a-2.b:	Against Applicant
GUIDELINE M (USE OF INFORMATION TECHNOLOGY):	AGAINST APPLICANT
Subparagraph 3.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