DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 24-00802
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Cynthia Ruckno, Esq., Department Counsel
For Applicant: *Pro se*

05/06/2025

Decision

FOREMAN, LeRoy F., Administrative Judge:

This case involves security concerns raised under Guidelines E (Personal Conduct) and M (Use of Information Technology). Clearance is granted.

Statement of the Case

Applicant submitted a security clearance application (SCA) on February 14, 2022. On August 15, 2024, the Defense Counterintelligence and Security Agency (DCSA) sent him a Statement of Reasons (SOR) alleging security concerns under Guidelines E and M. The DCSA acted under Executive Order (Exec. Or.) 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) promulgated in Security Executive Agent Directive 4, *National Security Adjudicative Guidelines* (December 10, 2016), which became effective on June 8, 2017.

Applicant answered the SOR on September 9, 2024. and requested a decision on the written record in lieu of a hearing. Department Counsel submitted the Government's written case on December 9, 2024. A complete copy of the file of relevant material (FORM) was sent to Applicant, who was given an opportunity to file objections and submit material to refute, extenuate, or mitigate the Government's evidence. He received the FORM on January 20, 2025, and submitted a response on February 20, 2025, which has been marked as Applicant's Exhibit (AX) A and admitted without objection. The case was assigned to me on April 2, 2025.

The FORM consists of six items. Items 1 and 2 are the pleadings in the case. Items 3 through 6 are the Government's evidence in support of the allegations in the SOR, Applicant did not object to Items 3 through 6, and they are admitted in evidence.

Findings of Fact

In Applicant's answer to the SOR, He denied the allegations in SOR ¶¶ 1.a and 1.b and admitted the allegation in SOR ¶ 2.a. His admissions are incorporated in my findings of fact.

Applicant is 49 years old. He is unmarried and has no children. He received an associate degree in May 1998 and a cyber security management certificate in January 2021. He worked as an information security and data protection specialist for a defense contractor from September 2005 to April 2021. He was unemployed from May 2021 to February 2022. He is currently employed by a defense contractor as a senior principal cyber information systems security analyst. He received a security clearance in April 2017.

In May 2021, Applicant was terminated from employment after a forensic audit of his computer reflected that he had accessed gaming and shopping sites during work hours during the period from January 12 through 18, 2021, resulting a total of 83.58 hours of unworked time being billed to a U.S. Government contract. (Item 6) The written termination notice stated, "It has been determined that you were using company resources and engaging in personal/not-work-related computer and internet usage during work hours." Applicant declined to sign the receipt for the written notice. (Item 5 at 17)

The record does not reflect how the hours of unworked time were computed. In Applicant's response to the FORM, he challenged the computation of 83.58 hours of unworked time, pointing out that he works a 40-hour week, was not authorized to work overtime hours or on weekends, and could not have billed 83.58 hours during the seven-day period that was audited.

In early February 2022, Applicant received an offer for a conditional appointment as a principal cyber information systems security analyst. When he submitted his SCA on February 14, 2022, he disclosed that he was fired from a previous job. He also disclosed that his previous job location was transferred from the West Coast to the East Coast, and that he had accepted another offer of employment, but it "fell through" after he accepted it. (Item 3 at 10-13)

When Applicant was interviewed by a security investigator on July 22, 2022, the investigator asked him about his previous termination of employment, Applicant stated that he was terminated for violation of company policy, but that he did not know what specific policy was violated. He told the investigator that he had informed his employer that he was unwilling to move to the new geographical location, and he suggested that his unwillingness to relocate may have been the reason for his termination. When the investigator confronted him with evidence that he was terminated for misuse of company time and unauthorized personal use of computer time and internet access, he immediately agreed and explained he was fired for listening to streaming music on an unclassified computer while working, which he thought was permissible because his employer allowed limited personal use of company computers. (Item 4 at 4; Item 6) He told the investigator that he did not contest his termination because he did not intend to move to the new geographical location. (Item 4 at 4)

In Applicant's answer to the SOR, he stated that he did not falsify material facts during his security interview because he did not have the termination notice with him during the interview and remembered only that he was terminated for a policy violation. He expressed regret for his personal misuse of company computers. He submitted a statement from a coworker, who has known him for more than 12 years. The coworker attests to his reliability, leadership, integrity and "can-do" attitude. (SOR attachments)

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.

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, 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 all available and reliable information about the person, past and present, favorable and unfavorable.

The Government reposes a high degree of trust and confidence in persons with access to classified information. This relationship transcends normal duty hours and endures throughout off-duty hours. Decisions include, by necessity, consideration of the possible risk 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. *See Egan* at 531. Substantial evidence is "such relevant evidence as a reasonable mind might accept as adequate to support a conclusion in light of all the contrary evidence in the same record." See ISCR Case No. 17-04166 at 3 (App. Bd. Mar. 21, 2019) It is "less than the weight of the evidence, and the possibility of drawing two inconsistent conclusions from the evidence does not prevent [a Judge's] finding from being supported by substantial evidence." *Consolo v. Federal Maritime Comm'n,* 383 U.S. 607, 620 (1966). "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. ISCR Case No. 15-01253 at 3 (App. Bd. Apr. 20, 2016).

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* 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* at 531.

Analysis

Guideline E, Personal Conduct

SOR ¶ 1.a alleges that Applicant was terminated from employment for engaging in personal/non-work-related computer and internet usage during work hours, resulting in a misuse of company time. SOR ¶ 1.b alleges that Applicant falsified material facts during a personal subject interview by deliberately seeking to conceal the information in SOR ¶ 1.a.

The security concern under this guideline is 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. Of special interest is any failure to

> cooperate or provide truthful and candid answers during national security investigative or adjudicative processes. . . .

The evidence in the FORM is sufficient to raise the following disqualifying condition under this guideline:

> AG ¶ 16(b): refusal to provide full, frank, and truthful answers to lawful questions of investigators, security officials, or other official representatives in connection with a personnel security or trustworthiness determination.

In the FORM, Department Counsel argued that the following disqualifying condition is also applicable:

> AG ¶ 16(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 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: . . .(3) a pattern of dishonesty or rule violations; and (4) evidence of significant misuse of Government or other employer's time or resources . . . .

This disqualifying condition is not applicable, because Applicant's conduct for which he was fired is explicitly covered under Guideline M, discussed below.

The following mitigating conditions under Guideline E are potentially applicable:

> AG ¶ 17(a): the individual made prompt, good-faith efforts to correct the omission, concealment, or falsification before being confronted with the facts; and

> AG ¶ 17(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.

AG ¶ 17(a) is established. Applicant initially suggested to the investigator that he was fired because of his unwillingness to relocate. However, as the interview continued and the investigator confronted him with information about the reasons for his termination, he immediately agreed that misuse of his computer and internet access was the reason for his termination. While he equivocated at the outset of the interview, he quickly acknowledged the reason for his termination. His prompt acknowledgment satisfies the underlying purpose of AG ¶ 17(a).

AG ¶ 17(c) is established. Falsification during the adjudication of an application for a security clearance is not minor. To the contrary, it "strikes at the heart of the security

clearance process." ISCR Case No. 09-01652 (App. Bd. Aug. 8, 2011.) However, in this case it was infrequent, occurred almost three years ago, and occurred under unique circumstances, while Applicant was trying to recover from a termination that he felt was unfair after 15 years of employment. Finally, Applicant has been chastened by this experience, and it is unlikely to recur.

Guideline M, Use of Information Technology

The concern under this Guideline is 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.

Applicant's admissions and the evidence in the FORM are sufficient to establish the following disqualifying condition in AG ¶ 40(e): "unauthorized use of any information technology system."

The mitigating condition in AG ¶ 41(a) is relevant: "so much time has elapsed since the behavior happened, or it happened under such unusual circumstances, that it is unlikely to recur and does not cast doubt on the individual's reliability, trustworthiness, or good judgment." This mitigating condition is established. Applicant's misuse of information technology occurred during a seven-day period in January 2021, more than four years ago, and there is no evidence of recurrence. Applicant has learned from the experience, and it is unlikely to recur.

Whole-Person Analysis

Under AG ¶ 2(c), the ultimate determination of whether to grant a security clearance must be an overall commonsense judgment based upon careful consideration of the guidelines and the whole-person concept. An administrative judge must evaluate an appellant's security eligibility by considering the totality of the appellant's conduct and all the relevant circumstances. An 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.

I have incorporated my comments under Guideline E and M in my whole-person analysis and applied the adjudicative factors in AG ¶ 2(d). Because Applicant requested a determination on the record without a hearing, I had no opportunity to evaluate his credibility and sincerity based on demeanor. *See* ISCR Case No. 01-12350 at 3-4 (App. Bd. Jul. 23, 2003). After weighing the disqualifying and mitigating conditions under Guidelines E and M and evaluating all the evidence in the context of the whole person, I conclude Applicant has mitigated the security concerns raised by his unauthorized use of an information technology system and his momentary lack of candor during an interview by a security investigator.

Formal Findings

I make the following formal findings on the allegations in the SOR:

Paragraph 1, Guideline E:	FOR APPLICANT
Subparagraphs 1.a and 1.b:	For Applicant
Paragraph 2, Guideline M:	FOR APPLICANT
Subparagraph 2.a:	For Applicant

Conclusion

I conclude that it is clearly consistent with the national security interests of the United States to grant Applicant eligibility for access to classified information. Clearance is granted.

LeRoy F. Foreman
Administrative Judge