DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 23-00525
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Daniel O'Reilley, Esq., Department Counsel
For Applicant: *Pro se*

01/30/2025

_____

Decision

_____

Curry, Marc E., Administrative Judge:

Applicant mitigated the financial considerations security concerns but failed to mitigate the security concerns governing use of information technology. Clearance is denied.

Statement of the Case

On May 20, 2023, the Department of Defense Counterintelligence and Security Consolidated Adjudications Service (DCSA CAS) issued a Statement of Reasons (SOR) to Applicant, detailing security concerns under Guideline F, financial considerations and Guideline M, use of information technology systems, explaining why it was unable to find it clearly consistent with the national interest to grant security clearance eligibility. The DCSA CAS took this action under Executive Order (EO) 10865, *Safeguarding Classified Information within Industry* (February 20, 1960), as amended; and DOD Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (January 2, 1992), as amended (Directive), and the National Security Adjudicative Guidelines (AG), effective June 8, 2017.

On June 8, 2023 Applicant answered the SOR, admitting the allegations and requesting a hearing, whereupon the case was assigned to me on April 2, 2024. On August 21, 2024, the Defense Office of Hearings and Appeals issued a notice of hearing, scheduling the case for September 19, 2024. The hearing was held as scheduled. I received four exhibits from the Government (Government Exhibit (GE) 1 – GE 4), and four exhibits from Applicant (Applicant exhibit (AE) A - AE D). At the parties' request, I left the record open to allow them to submit additional records. Within the time allotted, Department Counsel submitted two exhibits (GE 5 – GE 6), and Applicant submitted six exhibits (AE E and AE J) I admitted all of these exhibits into the record. The transcript (Tr.) was received on September 27, 2024**.**

Findings of Fact

Applicant is a 52-year-old single man with two children, ages 22 and 19. He is a high school graduate and earned approximately two years of college credit. He worked for various defense contractors during his career as a network engineer. His duties include protecting data security. (Tr. 94) Currently, he is senior network engineer and information security systems officer. Applicant is highly respected on the job. Over the years, he has earned several awards and accolades. (AE F) He has held a security clearance since 2001. (Tr. 37)

Applicant has a history of financial delinquencies, as alleged in the SOR. The debt alleged in subparagraph 1.a, totaling $8,683, is a delinquent credit card. Applicant fell behind on this bill after losing his job in June 2018 and being unemployed for four months. (Answer, Attachment (Att. 5) This debt prompted the creditor to file a claim against Applicant in 2023. (Answer, Att. 1) On March 31, 2023, the parties reached an agreement under which Applicant agreed to pay the balance in monthly $250 payments until satisfaction. (Answer, Att. 1 at 2) Applicant has been making the payments, as agreed.

Subparagraph 1.b, totaling $3,123, is a delinquent federal income tax bill from tax year 2018. Applicant satisfied this debt approximately 15 months ago, financing the balance with a loan.(GE D; Tr. 30)

Applicant did not file his tax year 2019 federal and state tax returns until February 2021, as alleged in subparagraphs 1.c and 1.d. He attributes his late filings to the COVID-related shutdowns. (Answer at 1) Now, all of his federal tax returns are current. (AE D) When he filed his state income tax return in February 2021, he received a $493 refund. (GE 2 at 59-60)

Applicant earns $147,000 annually. (Tr. 36) This is $30,000 more than he earned before his termination in 2017. (Tr. 25) He maintains a budget and has approximately $1,200 of monthly discretionary income, and $60,000 invested in a 401k plan. (Tr. 52 – 53)

In 2018, Applicant's then-contract employer was replaced by another contract employer. He remained at the same facility and continued to use the same workstation computer after the change. As part of the change in contractors, the previous contractor's

network had to be migrated to the corporate network of the new employer. (GE 2 at 68) As part of the migration, Applicant on June 18, 2018, in his capacity as the system administrator, tested the updated WiFi by connecting his workstation computer to the new WiFi network. Within 48 hours, he received a call from the information system security officer, who told him that content was being diverted from his workstation computer to servers in the People's Republic of China through a web browser developed by a Chinese company, and that Applicant had installed it on his work computer without authorization. (Tr. 67) His employer informed him that it would investigate the matter.

Applicant went on a scheduled vacation. When he returned to work on June 22, 2018, his employer informed him that the investigation was complete, and that he was being terminated. (GE 2 at 69)

Applicant admits installing the web browser on the computer. He had used it on the same computer with his previous employer, and nothing derogatory had ever been flagged. (Tr. 30, 64) When asked at the hearing why he used this relatively obscure browser owned by a Chinese company, instead of an employer-approved mainstream browser such as Internet Explorer or Google, Applicant explained that he could open new windows more quickly than he could with the mainstream web browsers. (Tr. 61) When pressed further about this explanation on cross-examination, Applicant agreed that the speed that the unauthorized browser opened windows was only nominally quicker than the mainstream browsers, saving him approximately ten to eleven seconds per day. (Tr. 90) He provided no other reason for using the unauthorized web browser. In 2022, Applicant was re-hired by the company that terminated him in 2018. (Tr. 27, 35)

Policies

The U.S. Supreme Court has recognized the substantial discretion the Executive Branch has in regulating access to information pertaining to national security, emphasizing that "no one has a 'right' to a security clearance." *Department of the Navy v. Egan*, 484 U.S. 518, 528 (1988). When evaluating an applicant's suitability for a security clearance, the administrative judge must consider the adjudicative guidelines. In addition to brief introductory explanations for each guideline, the adjudicative guidelines list potentially disqualifying conditions and mitigating conditions, which are required to be considered in evaluating an applicant's eligibility for access to classified information. These guidelines are not inflexible rules of law. Instead, recognizing the complexities of human behavior, these guidelines are applied together with the factors listed in the adjudicative process. The administrative judge's overall adjudicative goal is a fair, impartial, and commonsense decision. According to AG ¶ 2(c), the entire process is a conscientious scrutiny of a number of variables known as the "whole-person concept." The administrative judge must consider all available, reliable information about the person, past and present, favorable and unfavorable, in making a decision.

The protection of the national security is the paramount consideration. AG ¶ 2(b) requires that "[a]ny doubt concerning personnel being considered for national security eligibility will be resolved in favor of the national security." In reaching this decision, I have

drawn only those conclusions that are reasonable, logical, and based on the evidence contained in the record. Under Directive ¶ E3.1.14, the Government must present evidence to establish controverted facts alleged in the SOR. Under Directive ¶ E3.1.15, the applicant is responsible for presenting "witnesses and other evidence to rebut, explain, extenuate, or mitigate facts admitted by applicant or proven by Department Counsel. . .." The applicant has the ultimate burden of persuasion to obtain a favorable security decision.

A person who seeks access to classified information enters into a fiduciary relationship with the Government predicated upon trust and confidence. This relationship transcends normal duty hours and endures throughout off-duty hours. The Government places a high degree of trust and confidence in individuals to whom it grants access to classified information. 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. Section 7 of Executive Order 10865 provides that decisions shall be "in terms of the national interest and shall in no sense be a determination as to the loyalty of the applicant concerned." *See also* EO 12968, Section 3.1(b) (listing multiple prerequisites for access to classified or sensitive information).

Under the whole-person concept, the administrative judge must consider the totality of an applicant's conduct and all relevant circumstances in light of the nine adjudicative process factors in AG ¶ 2(d). They are as follows:

(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.

Analysis

Guideline F: Financial Considerations

Under this guideline, "failure to live within one's means, satisfy debts, and meet financial obligations may indicate poor self-control, lack of judgment, or unwillingness to abide by rules and regulations, all of which can raise questions about an individual's reliability, trustworthiness, and ability to protect classified or sensitive information." (AG ¶ 18) Applicant's history of delinquent debts triggers the application of AG ¶ 20(a), "inability to satisfy debts," and AG ¶ 20(c), "a history of not meeting financial obligations." Applicant's

failure to file his 2019 federal and state income tax returns on time triggers the application of AG ¶ 19(f), "failure to file . . . annual Federal, state, or local income tax returns or failure to pay annual Federal, state, or local income tax, as required."

Applicant's financial problems were not caused by foolish or profligate spending. Instead, they were caused by a four-month period of unemployment after he was terminated from his job in 2018. Conversely, he was he fired for cause after his employer discovered that he had installed an unauthorized browser on his workstation computer. As such, his job loss and the corresponding financial problems were not caused by circumstances beyond his control. Therefore, AG ¶ 20(b), "the conditions that resulted in the financial problem were largely beyond the person's control (e.g., loss of employment, a business downturn, unexpected medical emergency, a death, divorce or separation, clear victimization by predatory lending practices, or identity theft), and the individual acted responsibly under the circumstances," does not apply.

Nevertheless, Applicant is paying the commercial debt, alleged in subparagraph 1.a, he has satisfied his 2018 federal income tax delinquency, as alleged in subparagraph 1.b, is current on all his income tax filings, and has $1,200 of discretionary monthly expenses. Under these circumstances, I conclude that AG ¶ 20(d), "the individual initiated and is adhering to a good-faith effort to repay overdue creditors or otherwise resolve debts," and AG ¶ 20(g), "the individual has made arrangements with the appropriate tax authority to file or pay the amount owed and is in compliance with those arrangements," applies. I conclude Applicant mitigated the financial considerations security concerns.

Guideline M, Use of Information Technology

The security concerns generated by this guideline are set forth in AG ¶ 39, as follows:

> Failure to comply with rules, procedures, guidelines, or regulations pertaining to information technology systems may raise concerns about an individual's reliability and trustworthiness, calling into question the willingness or ability to properly protect sensitive systems, notebooks, and information. Information technology includes . . . any component, whether integrated into a larger system or not, such as hardware, software, or firmware, used to facilitate these transactions.

Applicant's installation of an unauthorized web browser on a work computer. application of the following disqualifying conditions under AG ¶ 40(e):

> (e) unauthorized use of any information technology system;
>
> (f) introduction . . . of hardware, firmware, software, or media to or from any information technology system when prohibited by rules, procedures, guidelines, or regulations, or when otherwise not authorized.

There is no record evidence that Applicant had ever misused information technology before the episode involving the unauthorized installation of a web browser on his work computer. He has not misused information technology since the 2018 episode. and is highly respected on his current job. Moreover, the employer that fired him in 2018 rehired him in 2022. These favorable facts raise the issue of whether the mitigating condition set forth in AG ¶ 41(a), "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," applies.

Despite the passage of time and the isolated nature of the episode, I remain troubled by Applicant's conduct. Security clearance adjudications are predictive judgments in which the adjudicator evaluates whether the nature, pattern, seriousness, and recency of an applicant's past transgressions generate an unacceptable risk that the applicant may engage in such conduct in the future, and that such future conduct could result in the compromise of classified, sensitive, or controlled unclassified information. In this case, what *could* happen as the result of irresponsible conduct, actually *did* happen as a result of irresponsible conduct. The nature and seriousness of Applicant's misuse of information technology was amplified by the fact that his job involved data security protection. Under these circumstances, the nature and seriousness of the conduct outweighs its isolated nature and the passage of time that has elapsed since the misuse of information technology. Under these circumstances, I conclude that Applicant has failed to mitigate the security concern.

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 F:	FOR APPLICANT
Subparagraphs 1.a – 1.d:	For Applicant
Paragraph 2, Guideline M:	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 interests of national security to grant Applicant eligibility for a security clearance. Eligibility for access to classified information is denied.

_____
Marc E. Curry
Administrative Judge