DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 20-01562
	)	
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Jeff Kent, Esq., Department Counsel
For Applicant: *Pro se*

October 5, 2021

_____

Decision

_____

GLENDON, John Bayard, Administrative Judge:

Applicant failed to mitigate security concerns regarding personal conduct, financial considerations, and use of information technology. Based upon a review of the pleadings and the documentary evidence, national security eligibility for access to classified information is denied.

Statement of the Case

On April 24, 2018, Applicant filed a security clearance application (SCA). On October 15, 2020, the Defense Counterintelligence and Security Agency, Consolidated Adjudications Facility (CAF), issued a Statement of Reasons (SOR) to Applicant detailing security concerns under Guideline E (personal conduct), Guideline F (financial considerations), and Guideline M (use of information technology). The CAF acted under Executive Order 10865, *Safeguarding Classified Information within Industry* (Feb. 20, 1960), as amended (Exec. Or.); Department of Defense (DoD) Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (Jan. 2, 1992), as amended

(Directive); and the adjudicative guidelines (AG) promulgated in Security Executive Agent Directive 4, *National Security Adjudicative Guidelines* (Dec. 10, 2016), effective within the DoD on June 8, 2017.

Applicant responded to the SOR (Answer). He admitted some of the facts alleged in the SOR, but ultimately denied each of the SOR allegations. Applicant requested a decision based upon the administrative (written) record without a hearing before an administrative judge of the Defense Office of Hearings and Appeals (DOHA).

On April 1, 2021, Department Counsel prepared and sent to Applicant a File of Relevant Material (FORM) with eight proposed exhibits, Items 1-8, attached thereto. Applicant received the FORM on April 5, 2021, and was advised that he had 30 days from the date of his receipt of the FORM to file any objections or to supply additional information or documents in response to the FORM. He did not object or submit anything further.

On July 16, 2021, the case was assigned to me. I have admitted into the record the evidentiary items attached to Department Counsel's FORM. The administrative form for Applicant to elect to have an in-person hearing or to request a decision based upon the administrative record without a hearing was missing from the file. Department Counsel subsequently provided the form reflecting Applicant's request for a decision based upon the administrative record. I have marked this form as Administrative Exhibit I.

Findings of Fact

Applicant's personal information is extracted from his SCA unless otherwise indicated by a parenthetical citation to the record. After a thorough and careful review of the pleadings, and the documentary evidence in the record, I make the following findings of fact.

Applicant is 35 years old and has worked for several defense contractors since 2004. He graduated from high school in 2003 and has taken some college courses. He was first granted a security clearance in 2006, which was renewed in 2011. He has never married and has no children.

The SOR allegations and the related details of each are set forth below:

Guideline E, Personal Conduct

1.a Unauthorized charges on corporate credit card - In his SCA, Applicant advised that he used his corporate credit card for personal charges and it became 90 days delinquent. He commented further he did not use the reimbursements he received from his employer for business expenses to pay down the debt on the credit card. He charged personal expenses during the period 2016 or 2017 to February 2018. Over time, the personal charges totaled about $19,750. At the time the debt became delinquent, he owed $9,990. He admitted his personal use of the credit card to his employer. His actions

violated company policy, and he received a final written warning on April 11, 2018 to pay the debt. He was ultimately able to repay the debt owed on the card with a loan from his father. (Item 3 at 34; Item 4 at 1; Item 7 at 6-7; Item 8.)

1.b. Unauthorized access to employer's teleconference calls after employment termination - In April 2018, Applicant was terminated by this employer due to his failure to submit his SCA in a timely fashion and other issues. His employer subsequently determined that after he had been terminated, Applicant had called in on a company conference line without authorization and listened to company-related business discussions without announcing his presence on the calls. The last time this happened was on August 29, 2018, and Applicant was questioned by the company's security department about his actions. (GE 4 at 2.)

In an incident report submitted by the company, a company official asserted that Applicant had admitted attempting to enter a conference call in a text to a company employee. The report also states that he admitted "calling into multiple program-based daily status meetings during the month of August 2018, including as recently as August 29, 2018." In his Answer, Applicant sought to dismiss the allegation as simply an accidental "pocket dial." He admitted using a former co-worker's access code, which was saved on Applicant's phone. He wrote that with the access code stored on his phone, it was possible to "speed dial" the number, even by accident, and enter the conference call. He claimed that he never listened to the calls and hung up when he realized his mistake. He has now deleted his former co-worker's conference number so that this mistake cannot happen again. (Item 2 at 1; Item 4 at 2; Item 7 at 7-8.)

I find Applicant's explanation about how he accidentally dialed into conference call at the time of company meetings to lack credibility. I conclude that his actions were deliberate.

Guideline F, Financial Considerations

2.a Loan account charged off in the amount of about $8,244 – In about 2015, Applicant opened this credit account to refinance a vehicle loan. He defaulted on his payments and the vehicle was repossessed in July 2017. The lender sold the debt to a collection agency. In his Answer, he denied the debt on the grounds that the debt was no longer owed to the original creditor identified in the SOR. This unpaid debt owed to the original lender is evidenced by the two credit reports attached to the FORM. (Item 2 at 2; Item 3 at 37;Item 5 at 2; Item 6 at 3-4; Item 7 at 11, 12.)

2.b Cross allegation of SOR 1.a – See above.

Guideline M, Use of Information Technology

3.a Cross allegation of SOR 1.b – See above.

In his Answer, Applicant wrote that his response to the SOR is "in no way deny[ing] these facts or circumstances." He realizes now that his lifestyle of working long hours, driving long daily commutes, eating out a lot and not taking care of his health was not working. He relocated and started a new job that would permit a healthier lifestyle. He is receiving financial advice from his father to improve his financial situation and repay his father for the loan described above. His father is a financial advisor. Applicant is focused on improving his health and lifestyle and wants to be able to have a family of his own. (Item 2 at 2.)

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.

Adverse clearance determinations 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*, 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. 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*, 484 U.S. at 531.

Analysis

Guideline E, Personal Conduct

The security concern under this guideline is set out in AG ¶ 15, which, in relevant part, provides, as follows:

> 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.

The following conditions under AG ¶ 16 have possible applicability to the facts of this case and may be disqualifying:

> (c) credible adverse information in several adjudicative issue areas that is not sufficient for an adverse determination under any 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 or sensitive information; and
>
> (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 of 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; and

(f) violation of a written or recorded commitment made by the individual to the employer as a condition of employment.

Assuming *arguendo* that Applicant's actions on August 30, 2018, are not sufficient for an adverse determination under any single guideline or that his actions are not explicitly covered under any other guideline and may not be sufficient for an adverse determination, then AG ¶¶ 16(c) and (d) have been established. The record evidence contains credible adverse information, which, when combined with all available information, supports a whole-person assessment of questionable judgment, untrustworthiness, unreliability, and unwillingness to comply with rules and regulations indicating that Applicant may not properly safeguard classified or sensitive information. Applicant's actions of misusing his company credit card while employed with the company and misusing its conference call system after being terminated constitute "a pattern . . . of rules violations" and a "significant misuse of. . . [his] employer's time and resources."

Furthermore, the evidence established the applicability of AG ¶ 16(f). His violation of his employer's credit card policy violated the commitment he made when he became an employee that he would comply with its policies. Such a commitment was a condition of his employment.

The guideline in AG ¶ 17 contains seven conditions that could mitigate security concerns arising from personal conduct. Two of these mitigating conditions have possible applicability to the facts of this case:

> (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.

AG ¶ 17(c) is not established. Applicant's behavior was not minor, remote in time, or infrequent. There was nothing unique about the circumstances of the behavior to

suggest that it is unlikely to recur. His actions cast doubt on his reliability, trustworthiness, and judgment.

AG ¶ 17(d) is only partially established. Applicant has acknowledged his misuse of his company credit card, but he has not acknowledged that he deliberately called in to company conference calls after his termination from the company. He has taken some steps to change his environment that caused him financial stress, but he has not had a sufficient track record of mature, responsible conduct to mitigate the security concerns raised under this guideline.

Guideline F, Financial Considerations

The security concern under this guideline is set out in AG ¶ 18 as follows:

> 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. . . . An individual who is financially overextended is at greater risk of having to engage in illegal or otherwise questionable acts to generate funds. . . .

This concern is broader than the possibility that a person might knowingly compromise classified information to raise money. It encompasses concerns about a person's self-control, judgment, and other qualities essential to protecting classified information. A person who is financially irresponsible may also be irresponsible, unconcerned, or negligent in handling and safeguarding classified information.

The following conditions under AG ¶ 19 that could be disqualifying:

(a) inability to satisfy debts;

(c) a history of not meeting financial obligations; and

(d) deceptive or illegal financial practices such as embezzlement, employee theft, check fraud, expense account fraud, mortgage fraud, filing deceptive loan statements and other intentional financial breaches of trust.

The record evidence established all three disqualifying conditions quoted above. Applicant's violation of his employer's trust by using his company credit card to finance large amount of personal expenses that he could not repay with his own funds is a form of deceptive financial practices falling under AG ¶ 19(d). His past-due debt on his vehicle loan established AG ¶¶ 19(a) and (c), especially when considered in conjunction with his company credit card actions over a period of a year or more.

The guideline in AG ¶ 20 contains seven conditions that could mitigate security concerns arising from financial difficulties. Four of these mitigating conditions have possible applicability to the facts of this case:

> (a) the behavior happened so long ago, was so infrequent, or occurred under such circumstances that it is unlikely to recur and does not cast doubt on the individual's current reliability, trustworthiness, or good judgment;
>
> (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;
>
> (c) the individual has received or is receiving financial counseling for the problem from a legitimate and credible source, such as a non-profit credit counseling service, and there are clear indications that the problem is being resolved or is under control; and
>
> (d) the individual initiated and is adhering to a good-faith effort to repay overdue creditors or otherwise resolve debts.

None of the above mitigating conditions have been established. Applicant's misuse of his employer's credit card to finance his personal expenses occurred sufficiently recently to cast doubt on his current reliability, trustworthiness, and judgment. The same is true with respect to his unpaid vehicle debt. Applicant has not established that the cause of his financial problems were conditions beyond his control. While he has repaid his employer for the funds he misappropriated, that repayment was funded by his father and is a unique situation. Applicant stated that he has received financial counseling from his father, but that counseling has not resulted in clear indications that Applicant's financial issues are under control. Applicant's failure to initiate a good-faith effort to repay his vehicle loan after the vehicle was repossessed four years ago is more representative of Applicant's lack of willingness to initiate and adhere to good-faith efforts to repay overdue creditors.

Guideline M, Use of Information Technology

The security concern under this guideline is set out in AG ¶ 39 as follows:

> 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.

The following conditions under AG ¶ 40 have possible applicability to the facts of this case and may be disqualifying:

(a) unauthorized entry into any information technology system;

(c) use of any information technology system to gain unauthorized access to another system or to a compartmented area within the same system; and

(e) unauthorized use of any information technology system.

The record evidence established that Applicant deliberately used his personal mobile device to access his former employer's conference calls using the access codes of one or more of his former co-workers. Such actions constitute both unauthorized entry into and unauthorized use of his former employer's information technology system in that the employer's conference calls are a computer-accessed, information technology system.

The guideline in AG ¶ 41 contains four conditions that could mitigate security concerns arising from financial difficulties. Two of these mitigating conditions have possible applicability to the facts of this case:

(a) so much time has elapsed since the behavior, or it has happened 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; and

(c) the conduct was unintentional or inadvertent and was followed by a prompt, good-faith effort to correct the situation and by notification to appropriate personnel.

Neither of the above mitigating conditions have been established. Applicant's use of his former employer's conference call information technology system occurred sufficiently recently to cast doubt on his current reliability, trustworthiness, and judgment. There is nothing in the record to suggest that the circumstances were unusual except for the fact that he did what he did, which casts doubt on his current reliability, trustworthiness, and judgment. Applicant's assertion that his actions were inadvertent is not credible. Moreover, he never made an effort to alert his former employer about his inadvertent "pocket dials" into company conference calls.

Whole-Person Analysis

Under AG ¶ 2(c), the ultimate determination of whether to grant or continue eligibility for a security clearance must be an overall commonsense judgment based upon

careful consideration of the guidelines and the whole-person concept. In applying the whole-person concept, an 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 and applying the adjudicative factors in AG ¶ 2(d), specifically:

> (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 Guidelines E, F, and M in my whole-person analysis and considered the adjudicative factors in AG ¶ 2(d). Additional comments are warranted. I have weighed Applicant's age and the lack of maturity evidenced by his actions. Also, I have considered his lack of remorse for his behavior. I acknowledge his statements that he has taken steps to improve his working and living conditions to create a healthier and more stable lifestyle and his efforts to become more financially responsible. He has not, however, established a sufficient track record of responsible conduct to mitigate the security concerns raised by the facts of this case.

Overall, the record evidence as described above leaves me with questions and doubts as to Applicant's eligibility and suitability for a security clearance. After weighing the applicable disqualifying and mitigating conditions and evaluating all of the evidence in the context of the whole person, I conclude Applicant has not mitigated the security concerns raised by his personal conduct, financial considerations, and use of information technology.

Formal Findings

Paragraph 1, Guideline E:	AGAINST APPLICANT
Subparagraphs 1.a and 1.b:	Against Applicant
Paragraph 2, Guideline F:	AGAINST APPLICANT
Subparagraphs 2.a and 2.b:	Against Applicant
Paragraph 3, Guideline M:	AGAINST APPLICANT
Subparagraph 3.a:	Against Applicant

Conclusion

I conclude that it is not clearly consistent with the national interests of the United States to grant Applicant national security eligibility for a security clearance. Eligibility for access to classified information is denied.

John Bayard Glendon
Administrative Judge