DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 22-02303
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Andre Gregorian, Esq., Department Counsel
For Applicant: *Pro se*

03/22/2024

_____

Decision

_____

RICCIARDELLO, Carol G., Administrative Judge:

Applicant failed to mitigate the security concerns under Guideline K, handling protected information and Guideline E, personal conduct. He successfully mitigated the Guideline F, financial considerations security concerns. Eligibility for access to classified information is denied.

Statement of the Case

On February 15, 2023, the Department of Defense issued to Applicant a Statement of Reasons (SOR) detailing security concerns under Guideline K, handling protected information, Guideline F, financial considerations and Guideline E, personal conduct. The action was taken under Executive Order (EO) 10865, *Safeguarding Classified Information within Industry* (February 20, 1960), as amended; DOD Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (January 2, 1992), as amended (Directive); and the adjudicative guidelines (AG) effective on June 8, 2017.

Applicant answered the SOR on March 15, 2023, and requested a hearing before an administrative judge. The case was assigned to me on January 9, 2024. I contacted

Applicant on January 11, 2024, and confirmed the date of hearing. The Defense Office of Hearings and Appeals (DOHA) issued a notice of hearing on January 17, 2024, scheduling the hearing by Microsoft Teams for January 31, 2024. I convened the hearing as scheduled. Applicant affirmatively waived the 15-day notice requirement. The Government offered exhibits (GE) 1 through 11. Applicant objected to GE 4, the summarized results of interviews. I sustained the objection. There were no other objections, and GEs 1 through 3 and 5 through 11 were admitted in evidence. Applicant and two witnesses testified on his behalf. He did not offer any exhibits at his hearing. I left the record open until February 14, 2024, to permit him to submit documents. Post-hearing, Applicant submitted documents that were marked Applicant Exhibits (AE) A through E. There was no objection, and they were admitted in evidence and the record closed. DOHA received the hearing transcript on February 9, 2024.

Findings of Fact

Applicant admitted the SOR allegations in ¶¶ 1.c, 1.d, 1.e, 1.g, 1.i, 1.j, 2.c, 2.d, 2.e, 2.g, 2.i, 2.j, 3.a, and 3.b. He denied SOR ¶¶ 1.a, 1.b, 1.f, 1.h, 2.a, 2.b, 2.f, and 2.h. His admissions are incorporated into the findings of fact. After a thorough and careful review of the pleadings, testimony, and exhibits submitted, I make the following findings of fact.

Applicant is 57 years old. He served in the Army National Guard from 1988 to 1998 and then the Army Reserve from 1998 to 2019 when he retired in the paygrade E-6. He was recalled to active duty from 2005 to 2007 and served in stateside posts. He married in 1992 and has two grown children. He earned a bachelor's degree in 2020. He has worked for federal contractors and other employers throughout his civilian career. He has held a security clearance since approximately 2008 while working for federal contractors and during his military career. (Tr. 33-37; GE 1, 2, 3)

In Applicant's June 2022 security clearance application (SCA) he listed his job title as "Cyber Security" from February 2015 to June 2020 for different employers. From September 2013 to March 2014, he was a systems administrator. (GE 1, 2, 3)

Applicant was employed by Company X, a federal contractor, from October 2019 until June 2020 when he was terminated. He held a security clearance while employed there. On his June 2022 SCA, he disclosed the termination and stated the reason he left this job was because "employment terminated didn't work out for myself." He also stated: "Bad fit didn't work out." He further disclosed that he was fired, and the reason was "auditing was incomplete a few systems didn't get audit for the week." In response to the question on whether he received disciplinary action or a warning, he disclosed an action occurred in February 2020, and he said the reason for the action was because "container was secured at the end of the day and my name was listed last[.] [I] didn't agree with the decision." (GE 3)

Applicant testified and confirmed that he was knowledgeable about the National Industrial Security Program Operating Manual (NISPOM), had new employee orientation from Company X, and had received training on its policies and security protocols.

Documents from Company X also state that he received training on the aspects of Company X's policies and procedures as it pertains to the NISPOM. It stated that he had received Information Systems (IS) training, retraining on ISs and shadowed by Compliance and Risk Assessor (CRA) and Information Systems Security Officer (ISSO) Ms. Y to ensure he was familiar with all IS and security protocols. The Government's evidence includes investigative reports for each alleged incident with the cited regulations from the NISPOM for reporting and safeguarding requirements for classified information. Applicant testified that he did not receive any training when he started working with Company X. He later admitted he was trained for the position he was hired. (Tr. 77,179-185; GE 6, 7, 8, 9)

The SOR alleged in ¶¶ 1.a through 1.j that Applicant committed security violations while at Company X. In Applicant's answer to the SOR and his testimony, he stated that the allegations in SOR ¶¶ 1.a and 1.d are for the same incident. The Government agreed. His admissions and explanations are as follows:

SOR ¶ 1.a alleged that in about January 2020, Applicant committed a security violation when he failed to properly secure an unclassified laptop computer at the end of the workday. SOR ¶ 1.d alleged he committed a security violation in about January 2020 when he left his badge in an unclassified computer overnight. He denied SOR ¶ 1.a and admitted ¶ 1.d. In his SOR answer, he said he only had a desktop computer and did not remember working on an unclassified laptop computer. He admitted he left his badge in his desktop computer overnight. He did not remember why he failed to retrieve it but surmised he was in a rush, and his actions were unintentional. He testified that when he returned to work the next day, he had to retrieve the badge from security personnel who found the badge the night before. The security officer made the report about the incident. Applicant did not report it to his supervisor. He testified that he was aware that it is against Company X's rules to leave your computer unattended with a badge inserted in it. He said he was aware it was a security violation, and it did not happen again. Applicant attributed his conduct to lack of training by his employer. I find SOR ¶ 1.d more accurately describes the incident. (Tr. 70-77, 83-91; GE 9)

SOR ¶ 1.b alleged that Applicant committed a security violation in about January 2020 when he failed to complete an open/close log for a secured area at the end of the workday. Applicant denied this allegation. In his SOR answer and his testimony, he stated that when entering a secured area, the first person in the area must make an entry in the logbook. Anyone who enters the area while the first person is still in the secured area does not have to make an entry in the logbook. The only other person required to make an entry in the logbook is the last person to leave the secured area. If the secured area is unoccupied later in the day and someone enters, they must make an entry in the logbook. Applicant denied this allegation because he said he was not the first person to enter the secured area, and he was not the last person to leave, so he was not required to make an entry in the logbook. He was familiar with the prescribed protocol. He said the Compliance and Risk Assessor (CRA) notified him that she was aware he was in the secured room, but he denied he was the last to leave. He stated that she could not have known who the last person was in the room. I was not provided evidence to show

Applicant was the last person to enter the secured room. I was only provided a one-line conclusion that said "Failure to complete the open/close log for a secured area" in Company X's General Administrative Inquiry/Security Violation report. There is insufficient evidence to find Applicant committed a security violation. (Tr. 91-108; GE 9)

SOR ¶ 1.c alleged that in about January 2020, Applicant committed a security violation by failing to secure a classified safe at the end of the workday. Applicant admitted this allegation in his SOR answer and stated he retrieved a laptop from the classified safe and then returned it. Later a security guard checked the safe and found the safe door was open and the combination knob had not been properly closed. Applicant said it was his first month on the job, and he may have accidentally not turned the knob enough times. He said it was unintentional and due to lack of training. He testified he believed he had turned the knob adequately, but maybe he did not. He then testified that perhaps someone after him had used the safe and did not turn the knob. His name was in the logbook as the last person to use the safe. He acknowledged that it was possible he did not secure the knob. Applicant could not recall if he received written disciplinary action. The next day he and coworkers were given refresher training for locking and securing security containers. Applicant provided conflicting testimony. I find Applicant committed a security violation. (Tr. 108-130; GE 5, 7, 9)

SOR ¶ 1.e alleged that in February 2020, Applicant brought his personal cell phone into a classified area. He was placed on a performance improvement plan. Another employee found the cell phone and reported it. In his SOR answer, Applicant admitted this allegation. He explained that he was unaware that the area outside of a secured room was also considered a classified area. He testified to get into this area that is outside of the secured room, he had to use a combination code to access it. He would then have to use another combination code to access the secure room. He said it was the first time he had accessed the area and was unfamiliar with it. The employee who found the phone reported the incident. Applicant did not report it to his supervisor because it had already been reported. I find this was a security violation. Applicant admitted he made a mistake. The violation was reported by his coworker. Applicant said his supervisor advised him he was on a performance improvement plan. He does not remember what it said. He said he thought it was an initial performance review that new employees receive. (Tr. 130-152; GE 9)

SOR ¶ 1.f alleged that in about May 2020, Applicant committed a security violation by failing to secure a classified safe and failing to perform an end-of-day security check. A classified safe was found unsecured and open for over four hours. Applicant was the last person to log opening the safe. Applicant gave the same explanation as he did for SOR ¶ 1.c that someone who did not properly log in could have opened the safe after him and be responsible. He denied he was required to perform an end-of-day security check as part of his responsibilities. There is insufficient evidence regarding whether it was part of Applicant's work responsibilities to do an end-of-day security check. There is substantial evidence to conclude Applicant committed a security violation by failing to properly secure the classified safe. He confirmed that the CRA discussed with him his negligence in leaving the safe open. (Tr. 152-179-185; GE 6, 7)

SOR ¶ 1.g alleged that in about May 2020, Applicant committed a security violation when he left an unclassified CD/DVD in a classified system. Applicant admitted this allegation in his SOR answer and said it was unintentional and inadvertent. He testified that he received an unclassified CD/DVD and loaded it into his computer and then forgot the disk was in the computer. Later someone found it and reported it. He admitted it was a security violation. (Tr. 185-187; GE 9)

SOR ¶ 1.h alleged that Applicant committed a security violation by failing to secure an unmarked DVD containing classified information. It was determined by his employer to be an act of gross negligence, and he was suspended. Applicant denied this allegation in his SOR answer and said he remembered leaving a DVD out but it was not labeled "unclassified" and he never put classified information on it. He denied he was suspended. Applicant testified that he was conducting an audit on his computer and his server was full. He took a blank DVD and formatted it, but said he never put it in the computer. The investigation determined that an unclassified DVD was found during an investigative audit and determined to be Applicant's responsibility. The DVD became classified when it was labeled. Applicant could not recall labeling it but said maybe he did. It was found in a classified system and determined to have been in the computer for three days prior to the audit. He further testified that he thought he left the disk on his desk and not in the computer drive. He admitted he was aware he should not leave a DVD in a classified system. He said he did not believe his conduct constituted gross negligence but was just a mistake. I find there is substantial evidence to conclude Applicant committed a security violation. (Tr. 187-206; GE 7, 8, 9; SOR answer)

SOR ¶ 1.i alleged that in about June 2020, Applicant committed a security violation when he failed to secure a laptop that contained classified information. His employer determined his conduct to be an act of gross negligence. Applicant admitted this security violation in his SOR answer. The investigation revealed that Mr. Q discovered Applicant's laptop sitting on top of a cabinet in front of Mr. Q's cubicle. He opened the laptop and discovered that it was a "Secret/NOFORN" (not releasable to foreign national) laptop, and no one was around to properly secure it. He instructed Applicant to come over and properly secure the laptop in the safe. Mr. Q asked Applicant why he left the laptop on the cabinet unattended because it was classified and should have been in his possession. Applicant's explanation to Mr. Q was he usually places the laptop on top of the safe after he has concluded his audit and then places it in the safe. He was at the safe with another employee acting as a second person verifier on the logbook, a new practice instituted. He signed the logbook. He forgot the laptop power cord and went to get it. He said while he was gone, Mr. Q must have come around the corner and saw the laptop. In the investigative report, Applicant said he was only gone for a minute. He said he could see over the cubicle, and no one came into the area. He said another employee was in the area, and he asked him to keep an eye on it. The other employee told the investigator that he did not hear Applicant ask him to watch the computer as he was in his cubicle and there was no one else in the area. Applicant was suspended after this incident. (Tr. 206-222; GE 9)

At this hearing Applicant, stated he could see the laptop at all times, and he was no more than five feet away from it. He said he believes that his superior thought he was too far away. He said he was unaware of how far away was permissible but thought it could be a hand-distance away. When asked about being "around the corner" he explained he could see the laptop above the divider. He said he took additional training and realized his mistake. I find Applicant committed a security violation. (Tr. 206-222; GE 9)

Audits on systems and computers were part of Applicant's job. The purpose of an audit is to monitor computers to ensure classified information is not compromised. It is an automated system that runs software that reviews what was accessed on that computer. The person responsible for an audit could be required to conduct an audit on 100 computers. Before doing an audit, the computers must be backed up. If a computer is turned off, it cannot be backed up and an audit cannot be accomplished. Applicant had several computers that he was responsible to audit, but they had not been backed up. When he ran the audit on the computers that he was responsible for, he could not conduct the audit on those that were not backed up. He was responsible to find the computers that had not been audited and conduct it. He failed to audit several computers. His employer terminated him in late June 2020 due to his inability to comply with company regulations and security procedures. Applicant admitted in his SOR answer this allegation. He explained that while conducting an audit of a computer he found that a disk was full, and he had to move files around to create space and thought a file got saved to a different location. He said he only missed doing the audit on one laptop. He testified that there were other employees that failed to do all of their audits. (SOR ¶ 1.j) (Tr. 77-83, 223-227; GE 9)

Applicant testified that he committed some security violations and denied others. He admitted he made mistakes. He believed he was not properly trained by his employer. He believed his supervisor was attempting to make him look bad. He said other employees committed similar offenses and were not written up or terminated. He testified that he has worked for other government contractors and did not have any security violations. (Tr. 229)

Throughout the hearing, Applicant was at times evasive and less than candid. He frequently changed his testimony when confronted with specific facts. Although some of his statements could be due to memory failure, I also believe at times his vague and nonresponsive statements were intentional.

The investigative inquiries report that Applicant received additional training after the first incident of leaving a safe unsecure (SOR ¶ 1.c). It also reported the corrective actions taken to preclude future violations were as follows:

> Rebriefing, retraining on procedures to safeguarding classified information via the Learning Management System and STEPP database, security providing discussion on security protocol, shadowing by ISSM [Information Systems Security Manager] or Compliance and Risk Assessor. (GE 8)

The SOR alleged that Applicant had two delinquent debts. He testified that in 2015 he was on a family reunion trip to Las Vegas. While there, he was approached by two people who attempted to sell him a timeshare (SOR ¶ 3.a - $7,123). He said he signed a contract and was told he could cancel it. They also signed him up for a credit card and put the downpayment for the timeshare on the credit card (SOR ¶ 3.b - $1,674). He denied that he signed up for this credit card and said he has never used it. Applicant credibly testified that he was told he could cancel the agreement within a couple of days, and he repeatedly attempted to do so within the time period but no one would answer the phone at the number he was provided. He never used the timeshare and never made payments. He said he has tried for years to resolve these debts. (Tr. 37-59; AE A-E)

In 2023, Applicant was contacted by two men about the timeshare. They invited him to dinner and told him that he could resolve the debt for the timeshare by taking out two credit cards and splitting the balance owed on each card. Applicant credibly testified that he was trying to take care of this debt that was on his credit report. He agreed to take out the two credit cards, which were supposed to resolve the timeshare debt, but they did not. He said each card was charged $3,000. He has been paying the amounts due on these credit cards. They are not alleged as being delinquent. Applicant disputed the debts on his credit report. His most recent credit report from January 2024 does not report the debts. He does not know if the two credit cards were actually used to pay the timeshare debt. He has no other delinquent debts. Post-hearing, he provided documents to show his efforts to dispute and resolve these debts. (Tr. 37-69; GE 11; AE A through E)

A former coworker and friend testified on Applicant's behalf. The coworker described Applicant as a person of integrity who always did the right thing. If he made a mistake, it was unintentional. He believed the employer was inconsistent in their warnings to employees for security violations. Some received verbal warnings for things that others, including Applicant, were written up for. His brother-on-law testified for him. He also served with him in the military. He believes Applicant did a great job while a soldier. They went to church together and Applicant is a man of character and is truthful. Applicant provided a narrative in his SOR answer. He said he is a family man and a trustee at his church. He volunteers at a facility for foster children. He was a youth coach for over ten years. He has never been arrested. (Tr. 238-254; SOR answer)

Policies

When evaluating an applicant's national security eligibility, the administrative judge must consider the AG. In addition to brief introductory explanations for each guideline, the adjudicative guidelines list potentially disqualifying conditions and mitigating conditions, which are used 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 in conjunction with the factors listed in the adjudicative process. The administrative judge's overarching 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. Likewise, I have avoided drawing inferences grounded on mere speculation or conjecture.

Under Directive ¶ E3.1.14, the Government must present evidence to establish controverted facts alleged in the SOR. Directive ¶ E3.1.15 states an "applicant is responsible for presenting witnesses and other evidence to rebut, explain, extenuate, or mitigate facts admitted by applicant or proven by Department Counsel, and has the ultimate burden of persuasion as to obtaining 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 reposes 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 an applicant may deliberately or inadvertently fail to safeguard classified information. Such decisions entail a certain degree of legally permissible extrapolation as to potential, rather than actual, risk of compromise of classified information.

Section 7 of EO 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).

Analysis

Guideline K, Handling Protected Information

The security concern for handling protected information is set out in AG ¶ 33:

> 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 an individual's trustworthiness, judgment, reliability, or willingness and ability to safeguard such information, and is a serious security concern.

AG ¶ 34 describes conditions that could raise a security concern and may be disqualifying. The following are potentially applicable:

(g) any failure to comply with rules for the protection of classified or sensitive information; and

(h) negligence or lax security practices that persist despite counseling by management.

There is substantial evidence[1] from Applicant's admissions and testimony, along with documents, that support he failed to comply with rules for the protection of classified or sensitive information and was lax or negligent in his security practices when he failed to secure a classified safe, left his badge in an unclassified computer overnight, took his cell phone into a classified area, left an unclassified CD/DVD in a classified system, failed to secure an unmarked DVD containing classified information, failed to properly secure a classified laptop computer, and failed to complete audits of systems as required (SOR ¶¶ 1.c through 1.j). Despite being trained and counseled by his employer the incidents persisted. The above disqualifying conditions apply.

Conditions that could mitigate handling protected information security concerns are provided under AG ¶ 35. The following is potentially applicable:

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

(b) the individual responded favorably to counseling or remedial security training and now demonstrates a positive attitude toward the discharge of security responsibilities ;

(c) the security violations were due to improper or inadequate training or unclear instructions; and

(d) the violation was inadvertent, it was promptly reported, there is no evidence of compromise, and it does not suggest a pattern.

Security violations are one of the strongest possible reasons for denying or revoking access to classified information, as they raise serious questions about an applicant's suitability for access to classified information. Once it is established that an applicant has committed a security violation, he or she has a very heavy burden of

[1] 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, e.g.,* ISCR Case No. 17-04166 at 3 (App. Bd. Mar. 21, 2019) (citing Directive ¶ E3.1.32.1). "This is something 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); ISCR Case No. 04-07187 at 5 (App. Bd. Nov. 17, 2006).

demonstrating that he or she should be entrusted with classified information. Because security violations strike at the very heart of the industrial security program, an administrative judge must give any claims of reform and rehabilitation strict scrutiny. In many security clearance cases, applicants are denied a clearance for having an indicator of a risk that they might commit a security violation (*e.g*., alcohol abuse, delinquent debts, or drug use). Security violation cases reveal more than simply an indicator of risk. *See* ISCR Case No. 03-26888 (App. Bd. Oct. 5, 2006).

I am cognizant of the heavy burden under this guideline. However, we are all human beings and mistakes will happen, even by the most careful of individuals. Applicant disclosed that he has worked in cyber security for several years. He was familiar with his duty to comply with the NISPOM and his employer's rules and regulations. He received training when he began his job. Some of security incidents did not require special training, such as ensuring the safe was locked and spinning the knob, ensuring you do not leave your badge in your computer overnight, leaving a DVD in a classified system and failing to secure a classified laptop. Other security violations may be unique to the employer, such as what area is considered a secured area where cell phones are prohibited. All of these are security incidents or violations that Applicant committed and demonstrate a pattern. I am unable to find his conduct was infrequent or happened under unusual circumstances and are unlikely to recur. AG ¶ 35(g) does not apply.

Applicant took some responsibility for his conduct, but also deflected it and offered alternative explanations for why he was not responsible. He cited his lack of training to be the reason for some of the security incidents, but also noted that he has held a security clearance for many years, was familiar with the NISPOM and had received training when he was hired. In addition, his years working as a cyber security analyst would indicate that he was aware or should have been aware of his duties to ensure a safe is properly closed, a badge is retrieved from your computer before leaving for the night, and classified laptops are not left unattended. The pattern of security violations indicates he failed to demonstrate a positive attitude toward the discharge of his security responsibilities. AG ¶¶ 35(b) and 35(c) do not apply.

Applicant's security violations were due to negligence. It appears that they were reported by other employees. The investigative reports indicate there was no compromise of classified information. However, there was clearly a pattern of security violations that cannot be overlook. AG ¶ 35(d) does not apply.

Guideline E: Personal Conduct

AG ¶ 15 expresses the security concern for personal conduct:

> 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 information. Of special interest is any failure to provide truthful and candid answers during the security clearance process or any other

> failure to cooperate with the security clearance process. The following will normally result in an unfavorable national security eligibility determination, security clearance action, or cancellation of further processing for national security eligibility:

AG ¶ 16 describes conditions that could raise a security concern and may be disqualifying. I find the following potentially applicable:

> (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 or sensitive information; and
>
> (e) personal conduct, or concealment of information about one's conduct, that creates a vulnerability to exploitation, manipulation, or duress by a foreign intelligence entity or other individual or group. Such conduct includes: (1) engaging in activities which, if known, could affect the person's personal, professional, or community standing.

Applicant's eight security incidents (SOR ¶¶ 1.c though 1.j) as alleged under Guideline K, were cross-alleged (SOR ¶ 2.a) under the personal conduct guideline. His conduct reflects questionable judgment and an unwillingness to comply with rules and regulations. It also created vulnerability to exploitation, manipulation, and duress. AG ¶ 16(e) is applicable. AG ¶ 16(c) is not perfectly applicable because Applicant's conduct is sufficient for an adverse determination under the handling protected information guideline. However, the general concerns about questionable judgment and an unwillingness to comply with rules and regulations contained in AG ¶¶ 15 and 16(c) are established.

AG ¶ 17 provides conditions that could mitigate security concerns. The following are potentially applicable:

> (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;
>
> (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; and

(e) the individual has taken positive steps to reduce or eliminate vulnerability to exploitation, manipulation, or duress.

Applicant's conduct was serious. He has not fully acknowledged his responsibility for his conduct, which raises concerns that he is not truly rehabilitated. I cannot find that future questionable conduct is unlikely to recur. His conduct continues to cast doubt on his current reliability, trustworthiness, and good judgment. None of the mitigating conditions, individually or collectively, are sufficiently applicable to overcome Applicant's conduct.

Guideline F: Financial Considerations

The security concern relating to the guideline for financial considerations is set out in AG ¶ 18:

> 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. Financial distress can also be caused or exacerbated by, and thus can be a possible indicator of, other issues of personnel security concern such as excessive gambling, mental health conditions, substance misuse, or alcohol abuse or dependence. An individual who is financially overextended is at greater risk of having to engage in illegal or otherwise questionable acts to generate funds. Affluence that cannot be explained by known sources of income is also a security concern insofar as it may result from criminal activity, including espionage.

AG ¶ 19 provides conditions that could raise security concerns. The following are potentially applicable:

(a) inability to satisfy debts; and

(c) a history of not meeting financial obligations.

Applicant has two delinquent debts associated with a timeshare he purchased in 2015. There is sufficient evidence to support the application of the above disqualifying conditions.

The guideline also includes conditions that could mitigate security concerns arising from financial difficulties. The following mitigating conditions under AG ¶ 20 are potentially applicable:

(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.

(e) the individual has a reasonable basis to dispute the legitimacy of the past-due debt which is the cause of the problem and provides documented proof to substantiate the basis of the dispute or provides evidence of actions to resolve the issue.

Applicant credibly testified that in 2015 he was the victim of predatory timeshare vendors who sold him property, required him to secure a credit card to pay the down payment and advised him he could cancel the contract within a couple of days. He attempted to cancel it within the time period and could not reach the company because they would not respond to his attempts. He then was approached about taking out two new credit cards to pay for the timeshare. Wanting to resolve the debts, he complied with the plan. He is making payments on those credit cards. For years he has been attempting to resolve the debts associated with the timeshare and credit card. He produced sufficient documentary evidence to show his efforts. The debts are no longer on his most recent credit report. I find he has acted responsibly, attempted to resolve the debts, and has a reasonable dispute. I find all of the above mitigating conditions apply.

Whole-Person Concept

Under the whole-person concept, the administrative judge must evaluate an applicant's eligibility for a security clearance by considering the totality of the applicant's conduct and all the circumstances. The 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.

Under AG ¶ 2(c), the ultimate determination of whether to grant eligibility for a security clearance must be an overall commonsense judgment based upon careful consideration of the guidelines and the whole-person concept.

I considered the potentially disqualifying and mitigating conditions in light of all the facts and circumstances surrounding this case. I have incorporated my comments under Guidelines K, E, and F in whole-person analysis. Some of the factors in AG ¶ 2(d) were addressed under those guidelines, but some warrant additional comment.

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." Applicant has not met his burden of persuasion. The record evidence leaves me with serious questions and doubts as to Applicant's eligibility and suitability for a security clearance. For these reasons, I conclude Applicant failed to mitigate the security concerns arising under Guideline K, handling protected information and Guideline E, personal conduct. He successfully mitigated the security concerns under Guideline F, financial considerations.

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 K:	AGAINST APPLICANT
Subparagraphs 1.a-1.b:	For Applicant
Subparagraphs 1.c-1.e	Against Applicant
Subparagraph 1.f:	Against Applicant (except failing to perform end-of-day security checks)
Subparagraphs: 1.g-1.j:	Against Applicant
Paragraph 2, Guideline E:	AGAINST APPLICANT
Subparagraph 2.a:	Against Applicant
Paragraph 3, Guideline F:	FOR APPLICANT
Subparagraphs 3.a-3.b:	For Applicant

Conclusion

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

_____
Carol G. Ricciardello
Administrative Judge