



**DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS**



In the matter of:)	
)	
[Redacted])	ISCR Case No. 16-03988
)	
Applicant for Security Clearance)	

Appearances

For Government: Nicole A. Smith, Esq., Department Counsel
For Applicant: Anthony J. Kuhn, Esq.

04/13/2018

Decision

FOREMAN, LeRoy F., Administrative Judge:

This case involves security concerns raised under Guidelines M (Use of Information Technology) and E (Personal Conduct). Eligibility for access to classified information is denied.

Statement of the Case

Applicant submitted a security clearance application on January 17, 2016. On May 15, 2017, the Department of Defense Consolidated Adjudications Facility (DOD CAF) sent him a Statement of Reasons (SOR) alleging security concerns under Guidelines M and E. The DOD CAF acted under Executive Order (Exec. Or.) 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) implemented by the DOD on September 1, 2006.¹

¹ Security Executive Agent Directive 4 (SEAD 4) was issued on December 10, 2016, revising the 2006 adjudicative guidelines for all adjudicative decisions issued on or after June 8, 2017. The changes resulting from issuance of SEAD 4 did not affect my decision in this case

Applicant answered the SOR on June 6, 2017, and requested a hearing before an administrative judge. Department Counsel was ready to proceed on July 20, 2017, and the case was assigned to me on December 13, 2017. On January 3, 2018, the Defense Office of Hearings and Appeals (DOHA) notified Applicant that the hearing was scheduled for January 24, 2018. I convened the hearing as scheduled. Government Exhibits (GX) 1 through 6 were admitted in evidence without objection. Applicant testified, presented the testimony of one witness, and submitted Applicant's Exhibits (AX) A through I, which were admitted without objection. DOHA received the transcript (Tr.) on January 31, 2018.

Findings of Fact²

In Applicant's answer to the SOR, he admitted the allegations in SOR ¶¶ 1.a, 2.d, and 2.g. He admitted the allegations in SOR ¶¶ 2.a-2.c, 2.e, and 2.f in part. His admissions in his answer and at the hearing are incorporated in my findings of fact.

Applicant is a 67-year-old employee of a federal contractor. He worked for other federal contractors from 1982 to 1985, 2000 to 2002, and 2003 to 2016, and he held a security clearance during each of those employments. (GX 3.)

Applicant served as a U.S. Army officer on active duty from May 1972 to March 1976. He successfully completed several rigorous military training courses. (AX G.) His efficiency report for his performance as a platoon leader, holding the rank of second lieutenant, placed him in the "excellent" category and recommended promotion along with his contemporaries. (AX I at 2-3.) His efficiency report rating him as section leader, holding the rank of first lieutenant, rated him in the "excellent" category and recommended promotion along with his contemporaries. (AX I at 5-6.) His efficiency report rating him as a company executive officer, holding the rank of first lieutenant, rated him as "superior" (the second highest rating) and recommended promotion ahead of his contemporaries. (AX I at 8-9.)

In June 1975, Applicant was arrested for shoplifting a magazine containing photographs of nude adult women from the Post Exchange. He resigned in lieu of trial by court-martial and received a general discharge under honorable conditions. His arrest and resignation are alleged in SOR ¶ 2.g.

At the hearing, Applicant admitted that he took the magazine and tried to leave the Post Exchange without paying for it. He testified that he was embarrassed and did not want to peruse it in the presence of women and children, and he intended to take it outside, look at it in his car, and return it. As he left with the magazine under his coat, he was apprehended. (Tr. 26-27.) He testified that he did not pay for the magazine

² Applicant's personal information is extracted from his security clearance application (GX 1) unless otherwise indicated by a parenthetical citation to the record.

because he would have been embarrassed to be seen holding the magazine as he paid for it. (Tr. 53-54.)

When Applicant submitted his SCA, he listed his discharge from the Army as “general,” and he listed the reason for his discharge as “obligation completed.” (GX 1 at 11.) When he was interviewed by a security investigator in July 2016, he admitted that he resigned his commission after being charged with shoplifting. He said that he did not know why he listed the reason for his discharge as “obligation completed.” (GX 2 at 15-16.) In response to DOHA interrogatories in February 2017, he disclosed that he resigned in lieu of court-martial, but he stated that he believed that “obligation completed” was the correct reason for the termination of his military service. (GX 2 at 6, 10.) At the hearing, he admitted that he did not complete his five-year service obligation, and it would not have been completed until May 1977. (Tr. 29.)

From February 2003 to September 2015, Applicant worked for a federal contractor supporting another government agency (AGA).³ From June 2015 to September 2015, Applicant used the AGA’s computer to view nude photographs of adult women. He testified that he looked for websites containing images of nude women about ten times in three months. (Tr. 56.) While he was at his desk, investigators from the AGA entered his office and asked if he was viewing inappropriate images. He told them he was, and they took the hard drive from his computer. A few minutes later, his supervisor took his security badge and told him to go home. (Tr. 15-16.) His access to the computer network was terminated by the AGA in September 2015, and the AGA told Applicant’s employer that his services were no longer needed. (GX 6.) His employer told him by email that he was on unpaid administrative leave until further notice. (Tr. 18.)

Applicant testified that, after several months, he orally told his employer’s vice-president that he was resigning. He testified that he believed that this conversation terminated his employment. He was unsure of the date of his conversation with the vice-president. He testified that he thought it was in April but it could have been earlier in February 2016. (Tr. 19.)

In Applicant’s answer to the SOR, two follow-up interviews by security investigators in July and August 2016, responses to interrogatories, and at the hearing, he denied that he was fired. Documentation from the AGA reflects that it terminated Applicant’s position as a contract employee supporting the AGA in September 2015. (GX 6.) Applicant has consistently stated that he was awaiting another assignment from his employer when he resigned. (GX 2 at 9, 14, 20.) His employer’s internal records reflect that he was terminated in January 2016, but there is no evidence in the record reflecting that he was notified of his termination. Applicant’s termination is alleged in SOR ¶ 1.a and cross-alleged in SOR ¶¶ 2.e and 2.f.

When Applicant submitted his SCA on January 17, 2016, he stated that he had been employed from February 2003 to “present,” and he did not disclose that he left this

³ By mutual agreement, the Directive applies to at least 20 other federal government agencies.

job four days earlier, on January 13, 2016. His answer to this question is alleged to be false in SOR ¶ 2.b. At the hearing, he testified that he believed he was still employed by his former employer when he submitted his SCA, and that he intended to tell his former employer if he found a new job. (Tr. 48-49.)

In the same SCA, Applicant answered “No” to questions whether, in the last seven years preceding his SCA, he (1) was fired; (2) quit after being told he would be fired; (3) left a job by mutual agreement following charges or allegations of misconduct; (4) left a job by mutual agreement after notice of unsatisfactory performance; or (5) received a written warning, been officially reprimanded, suspended, or disciplined for misconduct in the workplace, such as a violation of security policy. His failure to disclose his termination for misuse of the AGA’s computer is alleged in SOR ¶ 2.c.

When Applicant was interviewed by a security investigator in July 2016, he stated that he resigned from his employment because his employer could not find work for him. He also stated that he did not receive any written warnings, official reprimands, suspensions, or disciplinary actions from his employer as a result of his misuse of the AGA’s computer. (GX 2 at 14-15.)

At the hearing, Applicant testified that he did not believe he was fired or left his employment by mutual agreement following charges or allegations of misconduct. (Tr. 57.) When asked if he believed he was disciplined or reprimanded when the AGA terminated his services and his employer suspended him without pay, he responded:

It certainly can be perceived to be and now that I look back on it, I’d say yeah, that’s --- I probably should have responded to that particular interrogatory that [it] was punishment. . . . At the time, I didn’t really think that [it] was punishment and I really didn’t give it a lot of thought.

He denied attempting to mislead anyone by answering “No” to the employment questions. (Tr. 23.) His failures to disclose his suspension in his SCA and during the July 2016 security interview are not alleged in the SOR.

In the same SCA, Applicant answered “No” to a question asking whether, in the last seven years, he had introduced, removed, or used hardware, software, or media in connection with any information technology system without authorization, when specifically prohibited by rules, procedures, guidelines, or regulations or attempted any of the above. When questioned by a security investigator in August 2016, Applicant told the investigator that he had misread the question and should have answered “Yes.” (GX 2 at 20.) SOR ¶ 2.d alleges his failure to disclose his misuse of the AGA’s computer in response to this question.

Applicant admitted SOR ¶ 2.d in his answer to the SOR. However, at the hearing, he testified that he thought the question about misusing technology systems involved “misusing the hardware and software, introducing hardware, introducing software that would damage their equipment.” He admitted that he misused the AGA’s information

technology system in the sense that “there were regulations [and] they told us that you should not be viewing anything inappropriate on your computer.” (Tr. 25.)

Applicant’s performance review from his former employer for 2015 rated him as meeting expectations in six performance categories, exceeding expectations for teamwork, and exceeding expectations for productivity. (AX H at 1.) His performance reviews for 2013 and 2014 rated him as often exceeding expectations (the second highest rating) in all categories except productivity, for which he was rated as consistently exceeding expectations (the highest rating) and adherence to company policies and procedures, for which he was rated as meeting expectations (the middle rating). (AX H at 2-6.)

Applicant’s wife has known him for 47 years and they have been married for 44 years. She is well educated and has extensive experience working as a management consultant for federal contractors. She has held a security clearance while working on several federal contracts. She and Applicant worked together on a two-year federal contract. She considers Applicant honest, trustworthy, and kind. She testified that Applicant is “totally incapable of lying.” She corroborated Applicant’s testimony about his uncertainty about his employment status after he was caught viewing inappropriate material on his work computer. She corroborated his testimony about his uncertainty regarding his answers to questions in the SCA. She was hurt by his viewing of nude women, but she has forgiven him and considers that conduct totally out of character for him. (Tr. 70-101.)

Applicant submitted numerous testimonials to his good character, truthfulness, honesty, and suitability for a security clearance. The testimonials were submitted by a neighbor, who worked for the Army for 30 years and has known Applicant and his wife since 2003 (AX A), former co-workers (AX B; AX E; AX F), and former supervisors (AX C; AX D).

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*, 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 M, Use of Information Technology (IT)

SOR ¶ 1.a alleges that Applicant used the AGA's computer to view "pornography"⁴ and the AGA removed him from the work site and terminated his "security access."

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 documentary evidence submitted at the hearing establish the following potentially disqualifying condition: AG ¶ 40(e) ("unauthorized use of any information technology system"). However, the disqualifying condition in AG ¶ 40(f) ("introduction, removal, or duplication 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") is not established. This language of this disqualifying condition is almost identical to the question in Applicant's SCA, to which he answered "No." His answer to the question was correct, because the evidence reflects that Applicant did not introduce, remove, or duplicate any hardware, firmware, software, or media into his computer. He simply used the existing system to open and view websites containing inappropriate material.

The relevant mitigating condition is 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"). Applicant's misuse of his workplace computer happened about two and a half years ago, but it did not happen under unusual circumstances. There are no "bright line" rules for determining when conduct is mitigated by passage of time. The determination must be based on a careful evaluation of the totality of the evidence. See ISCR Case No. 02-24452 at 6 (App. Bd. Aug. 4, 2004). If the evidence shows "a significant period of time has passed without any evidence of misconduct," then an

⁴ It is not clear from the record whether the images of adult nude women viewed by Applicant constituted "pornography." However, the record reflects that the images were inappropriate material that was prohibited on the AGA's work computers.

administrative judge must determine whether that period of time demonstrates “changed circumstances or conduct sufficient to warrant a finding of reform or rehabilitation.” *Id.*

Applicant did not voluntarily stop his unauthorized viewing of inappropriate material. He gained access to and viewed inappropriate material about ten times in a three-month period. He stopped because he was caught. He has been under pressure to regain his security clearance from September 2015, when he was caught, until the present. Finally, as discussed below under Guideline E and in my whole-person analysis, he has not been completely candid during the security clearance process, and his lack of candor diminishes the weight of the evidence of rehabilitation. Under these circumstances, I am not satisfied that sufficient time has passed to mitigate his misuse of information technology.

Guideline E, Personal Conduct

The SOR alleges that Applicant deliberately failed to disclose his termination from employment in January 2016 during interviews with a security investigator in July and August 2016 (SOR ¶ 2.a). It also alleges that he falsified his SCA regarding his employment record (SOR ¶¶ 2.b and 2.c) by misrepresenting when his employment with a former employer ended and failing to disclose that he was terminated for misuse of IT systems. (SOR ¶ 2.d). It alleges that he was terminated for misuse of the AGA’s computer (SOR ¶ 2.e). It cross-alleges the conduct alleged in SOR ¶ 1.a (SOR ¶ 2.f). Finally, it alleges that he was arrested and charged with shoplifting a pornographic magazine in June 1975, resigned his commission, and received a general discharge under honorable conditions (SOR ¶ 2.g). The SOR does not allege Applicant’s mischaracterization of the reason for the termination of his military service in his SCA or his responses to DOHA interrogatories, nor does it allege Applicant’s failure to disclose in his SCA and in the July 2016 and August 2016 interviews that he was suspended and disciplined for misconduct.⁵

The 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. . . .

⁵ Conduct not alleged in the SOR may not be an independent basis for denying or revoking a security clearance, but it may be considered to assess an applicant’s credibility; to decide whether a particular adjudicative guideline is applicable; to evaluate evidence of extenuation, mitigation, or changed circumstances; to consider whether an applicant has demonstrated successful rehabilitation; or as part of a whole-person analysis. ISCR Case No. 03-20327 at 4 (App. Bd. Oct. 26, 2006). I have considered Applicant’s misstatement of the reason for the termination of his military service and his failure to disclose his suspension for misusing the AGA’s computer for these limited purposes.

The potentially following disqualifying conditions under this guideline are relevant:

AG ¶16(a): deliberate omission, concealment, or falsification of relevant facts from any personnel security questionnaire, personal history statement, or similar form used to conduct investigations, determine employment qualifications, award benefits or status, determine national security eligibility or trustworthiness, or award fiduciary responsibilities;

AG ¶16(b): deliberately providing false or misleading information; or concealing or omitting information, concerning relevant facts to an employer, investigator, security official, competent medical or mental health professional involved in making a recommendation relevant to a national security eligibility determination, or other official government representative;

AG ¶ 16(c): credible adverse information in several adjudicative issue areas that is not sufficient for an adverse determination under any other single guideline, but which, when considered as a whole, supports a whole-person assessment of questionable judgment, untrustworthiness, unreliability, lack of candor, unwillingness to comply with rules and regulations, or other characteristics indicating that the individual may not properly safeguard classified or sensitive information;

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 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;

AG ¶ 16(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; . . . and

AG ¶ 16(f): violation of a written or recorded commitment made by the individual to the employer as a condition of employment.

In this case, the applicability of the disqualifying conditions in AG ¶¶ 16(a) and 16(b) to SOR ¶¶ 2.a and 2.c (alleging failure to disclose that he was fired) is dependent

on whether Applicant knew he had been terminated on January 13, 2016, when he submitted his SCA four days later and when he was interviewed by a security investigator in July and August 2016. He knew that his relationship with the AGA was terminated, but he was told by his employer that he would be on unpaid administrative leave until further notice. While the internal communications among his former supervisors reflect that he was terminated on January 13, 2016, there is no evidence that he was informed of his termination until after he submitted his SCA and was interviewed by security investigators. He has consistently stated that he believed that he was still employed, albeit in an unpaid status, until he orally told a company official that he was resigning. Applicant's testimony on this issue was plausible and credible. I conclude that Applicant has refuted the allegations in SOR ¶¶ 2.a, 2.b, and 2.c, alleging intentional failure to disclose that he was terminated on January 13, 2016, for misuse of the AGA's computer.

Applicant admitted that the combination of being terminated by the AGA and suspended by his employer should have caused him to answer "Yes" to the question in Section 13C of his SCA regarding suspension or disciplinary action. However, the SOR does not allege this omission.

With respect to Applicant's failure to disclose his misuse of the AGA's computer in response to the question in his SCA asking if he had introduced, removed, or used hardware, software, or media in connection with any information technology system without authorization or when specifically prohibited, the evidence summarized in the above discussion of Guideline M indicates that Applicant had not "introduced, removed, or used hardware, software, or media." He simply used the existing system to access website containing images of nude adult women. His "No" answer to this question was correct. Thus, I conclude Applicant has refuted the allegation in SOR ¶ 2.d.

Applicant's arrest for shoplifting in 1975 and his misuse of the AGA's computer establish the disqualifying conditions in AG ¶¶ 16(c), 16(d), and 16(e). However, AG ¶ 16(f) is not established. Applicant admitted that he had been told not to access inappropriate material, but the record contains no evidence of a "written or recorded commitment" by Applicant to comply with the policy.

The following mitigating conditions are potentially relevant:

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 not applicable, because Applicant has refuted all the allegations of falsification alleged in the SOR ¶¶ 2.a-2.d. AG ¶ 17(c) is established for the 1975 shoplifting incident, which is mitigated by the passage of time. However, Applicant's recent false statement in his SCA about the consequences of the shoplifting incident raises concern about his credibility and diminishes the weight of the mitigating evidence regarding his misuse of the AGA's computer.

Whole-Person Concept

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. 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).⁶

I have incorporated my comments under Guidelines M and E in my whole-person analysis and applied the adjudicative factors in AG ¶ 2(d). Some of the factors in AG ¶ 2(d) were addressed under those guidelines, but some warrant additional comment. Applicant's arrest for shoplifting in 1975 is mitigated by the passage of time, but his misrepresentation of the consequences of his conduct are a concern. He falsely represented that he completed his service obligation, when in fact he left the Army in disgrace and did not complete his service obligation. He did not admit that he failed to complete his service obligation until the hearing.

Similarly, Applicant answered "No" to all the questions in his SCA about the consequences of his misuse of the AGA's computer. He did not disclose his suspension in his SCA, and he did not admit it until he was questioned about it at the hearing.

Applicant's efforts to parse the truth narrowly in his SCA fall short of full, frank, and candid answers to the questions in the SCA that are essential to the integrity of the industrial security program. See ISCR Case No. 01-03132 at 3 (App. Bd. Aug. 8, 2002). His lack of candor during the security-clearance process undercuts the evidence of rehabilitation after his repeated misuse of the AGA's computer.

Applicant's repeated misuse of the AGA's computer raised serious security concerns. "Once a concern arises regarding an applicant's security clearance eligibility, there is a strong presumption against the grant or maintenance of a security clearance." ISCR Case No. 09-01652 at 3 (App. Bd. Aug 8, 2011), *citing Dorfmont v. Brown*, 913

⁶ The factors are: (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.

F.2d 1399, 1401 (9th Cir. 1990), *cert. denied*, 499 U.S. 905 (1991). After weighing the disqualifying and mitigating conditions under Guidelines M and E, and evaluating all the evidence in the context of the whole person, I conclude Applicant refuted the allegations in SOR ¶¶ 2.a-2.d that he falsified his SCA, but he has not mitigated the security concerns raised by his misuse of an IT system.

Formal Findings

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

Paragraph 1, Guideline M (Use of IT): AGAINST APPLICANT

 Subparagraph 1.a: Against Applicant

Paragraph 2, Guideline E (Personal Conduct): AGAINST APPLICANT

 Subparagraph 2.a-2.d: For Applicant

 Subparagraph 2.e-2.f: Against Applicant

 Subparagraph 2.g: For Applicant

Conclusion

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

LeRoy F. Foreman
Administrative Judge