DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
[Redacted]	)	ISCR Case No. 22-01863
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Carroll Connelley, Esq., Department Counsel
For Applicant: *Pro se*

02/29/2024

_____

Decision

_____

FOREMAN, LeRoy F., Administrative Judge:

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

Statement of the Case

Applicant submitted a security clearance application (SCA) on November 8, 2017. On May 10, 2023, the Defense Counterintelligence and Security Agency Consolidated Adjudication Services (DCSA CAS) sent him a Statement of Reasons alleging security concerns under Guidelines K, M, and E. The DCSA CAS acted under Executive Order (Exec. Or.) 10865, *Safeguarding Classified Information within Industry* (February 20, 1960), as amended; Department of Defense (DOD) Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (January 2, 1992), as amended (Directive); and the adjudicative guidelines (AG) promulgated in Security Executive Agent Directive 4, *National Security Adjudicative Guidelines* (December 10, 2016).

Applicant answered the SOR on May 16, 2023, denied all the allegations, and requested a hearing before an administrative judge. Department Counsel was ready to

proceed on August 22, 2023, and the case was assigned to me on December 8, 2023. On December 19, 2023, the Defense Office of Hearings and Appeals (DOHA) notified Applicant that the hearing was scheduled to be conducted on January 30, 2024. I convened the hearing as scheduled. Government Exhibits (GX) 1 through 3 were admitted in evidence without objection. Applicant testified and submitted Applicant's Exhibits (AX) A and B, which were admitted without objection. I kept the record open until February 13, 2024, to enable him to submit additional documentary evidence. He timely submitted AX C through F, which were admitted without objection. DOHA received the transcript (Tr.) on February 6, 2024.

Findings of Fact

Applicant is a 36-year-old senior systems administrator employed by a federal contractor since September 2018. He received an associate degree from a technical institute in July 2008. He has never married and has no children.

Applicant worked in non-federal jobs after receiving his associate degree until he was hired by a federal contractor in July 2009. He received a security clearance in June 2009. From August 2009 to August 2012, he was assigned to duties as a contractor employee with U.S. Marines in an overseas location. While assigned to duty with the Marines, he was reprimanded by his civilian employer for his conduct on one occasion. The record does not reflect the conduct for which he was reprimanded. After his employer's contract ended in August 2012, he worked for other federal contractors. At the time he submitted his SCA, he had been working for a federal contractor since October 2017. He was terminated from this employment in August 2018 for reasons set out in the SOR, and he was hired by his current employer shortly thereafter.

Applicant's job description while working for his former employer as the senior systems administrator made him responsible for "ensuring the reliable operation of IT systems." His specific duties and responsibilities included providing server management of classified and unclassified networks; providing configuration, support, maintenance, and troubleshooting of systems, servers, and desktops; and establishing scripts to automate the team's infrastructure task, patching, and other operations duties. (GX- 3 at 20)

Applicant testified that his first year with his former employer went well, but after the leadership changed, several employees were replaced with outsiders who had worked for the new leadership. Because he did not believe that the new leadership understood the requirements of his job, he began searching for a new job. He accepted an offer from his current employer while still working for his former employer. (Tr. 15-16)

Applicant testified that on August 20, 2018, while he was still employed by his former employer, he was verbally informed by his immediate supervisor that he was being terminated because of his "hostile behavior" toward a senior executive of the company at a meeting two days earlier, by removing his glasses and rubbing his forehead while the senior executive was speaking. Applicant testified that he was upset at being terminated

and asked his supervisor what the real reason was for his termination. (Tr. 22) On the same day, he sent an email to his supervisor denying that he acted aggressively at the meeting with the senior executive. (AX F at 4)

On August 23, 2018, Applicant's supervisor sent him an email alleging eight concerns that had arisen since April 2018 and were the basis for his termination. Applicant testified that he did not receive this email, which was sent to his father's email address. (GX 3 at 2; Tr. 24) Five concerns were incorporated into SOR ¶¶ 1.a-1.e, alleging concerns under Guideline K. SOR ¶ 2.a cross-alleged the same five concerns under Guideline M. The eight concerns in the former employer's August 2018 email were copied verbatim into SOR ¶ 3.a, alleging personal conduct under Guideline E.

The August 2018 email did not describe the evidence on which the eight concerns were based. There is no evidence that the concerns were investigated before the email was sent to Applicant. The concerns were described in general terms in the email, and the SOR allegations incorporating them did not meet the specificity required by Directive ¶ E3.1.3 (SOR shall be a detailed and comprehensive as the national security permits). The evidence pertaining to the allegations in the SOR is summarized below.

SOR ¶ 1.a: Security threats (attempting to access systems without clearance (Concern #1). Applicant denied this allegation. The record contains no evidence of attempts by Applicant to access systems without a proper clearance.

SOR ¶ 1.b: Performing systems scans not within requested tasks or job duties (Concern #4). Applicant denied this allegation. The record contains no evidence of instances when Applicant performed systems scans that were not within his assigned duties.

SOR ¶ 1.c: Attempting to secure an administrator account for network devices without a top secret clearance (Concern #5). Applicant testified that he had no memory of requesting an administrator account for himself. He believed that he had all the access he needed to perform his job. (Tr. 31) In response to DOHA interrogatories, he stated that the only times he submitted requests for new administrative accounts was for new administrators joining the program. These requests were part of his duties as a senior administrator. (GX 3 at 3, 5)

SOR ¶ 1.d: Bringing a personal CD-ROM into the secure workplace (Concern #6). Applicant admitted this allegation. He testified that he had a personal CD-ROM in his gym bag, and he had forgotten that it was in his gym bag when he came to work. As soon as he discovered it, he turned it in to his supervisor, because he knew that bringing it into the workplace was a violation of his employer's rules. (Tr. 28-29)

SOR ¶ 1.e: Returning to the secure office environment after hours for a not verifiable or reasonable purpose (Concern #3). Applicant admitted returning to the office after hours for non-work purposes. He testified that there were occasions when he missed his bus during cold weather, and he returned to the office to wait for other

transportation. There were other team members still working while he was in the secure area. There is no evidence that he engaged in any suspicious activity while in the office. He testified that he was never told that he was forbidden to be in the office outside of his prescribed work hours. (Tr. 34)

SOR ¶ 2.a: Cross-alleges SOR ¶¶ 1.a-1.e under Guideline M. The evidence is the same as described above for SOR ¶¶ 1.a-1.e.

SOR ¶ 2.b: Termination from employment due to concerns in SOR ¶¶ 1.a-1.e. The evidence establishes that Applicant was terminated for the reasons set out in the SOR. However, only SOR ¶¶ 1.d and 1.e were supported by evidence in the record.

SOR ¶ 3.a: Terminated from employment for violations alleged in SOR ¶¶ 1.a-1.e, plus Concern #2 (Inability to mask emotions to the point of disrupting meetings), Concern #7 (Repeated attire and appearance issues), and Concern #8 (Aggressive behavior during a customer/co-worker meeting).

The record contains no evidence that Applicant disrupted meetings. When Applicant was questioned by a security investigator about disruptive behavior at work, he disclosed one occasion involving an exchange of words with a coworker about how to do a job. He considered it to be no more than a disagreement. (GX 3 at 13) The only evidence of "aggressive behavior" was the accusation of his supervisor that he engaged in aggressive behavior by removing his glasses and rubbing his head while a senior executive was speaking at a meeting. (Tr. 22) There is no evidence of the attire and appearance requirements for his job and no evidence that he was warned about inappropriate attire. To the contrary, a co-worker submitted a statement that Applicant always wore appropriate attire and that he wore a shirt and tie every day even though business casual was the norm. (AX A)

Two senior systems engineers employed by Applicant's former employer submitted statements rebutting the eight concerns about Applicant. One of them stated that if he had any doubts about Applicant's trustworthiness and professional behavior, he would not have submitted his statement of support. (AX A; AX B)

Applicant testified that his overseas service with the Marine Corps was stressful. In addition, his partner passed away in 2013. He believed that he was diagnosed by a psychiatrist with post-traumatic stress disorder. He is currently taking medication for attention deficit hyperactivity disorder (ADHD) and anxiety. (Tr. 35-38)

Applicant is highly regarded by his current employer. His senior program manager and program director each submitted letters commenting on his proficiency, rigorous adherence to information security, outstanding interpersonal skills, and ability to work within a team. (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 K (Handling Protected Information)

The concern under this guideline 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.

The allegations in SOR ¶¶ 1.a, 1.b, and 1.c are not supported by the evidence in the record. However, the allegations in SOR ¶¶ 1.d and 1.e are supported by the record and are sufficient to establish the disqualifying condition in AG ¶ 34(g): "any failure to comply with rules for the protection of classified or sensitive information." Applicant admitted that he violated the rules by bringing a personal CD-ROM into a protected area and that he sometimes returned to his secure work area for no purpose except personal convenience.

Two mitigating conditions are relevant:

> AG ¶ 35(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; and
>
> AG ¶ 35(d): the violation was inadvertent, it was promptly reported, there is no evidence of compromise, and it does not suggest a pattern.

Both mitigating conditions are established. More than five years have elapsed. The incident with the CD-ROM was inadvertent and promptly reported. Neither incident is likely to recur. The evidence does not suggest a pattern of security violations.

Guideline M, Use of Information Technology

The concern under this Guideline is set out in AG ¶ 39:

Failure to comply with rules, procedures, guidelines, or regulations pertaining to information technology systems may raise security concerns about an individual's reliability and trustworthiness, calling into question the willingness or ability to properly protect sensitive systems, networks, and information. Information Technology includes any computer-based, mobile, or wireless device used to create, store, access, process, manipulate, protect, or move information. This includes any component, whether integrated into a larger system or not, such as hardware, software, or firmware, used to enable or facilitate these operations.

The following disqualifying conditions are potentially relevant:

AG ¶ 40(a): unauthorized entry into any information technology system;

AG ¶ 40(b): unauthorized modification, destruction, or manipulation of, or denial of access to, an information technology system or any data in such a system;

AG ¶ 40(c): use of any information technology system to gain unauthorized access to another system or to a compartmented area within the same system;

AG ¶ 40(d): downloading, storing, or transmitting classified, sensitive, proprietary, or other protected information on or to any unauthorized information technology system;

AG ¶ 40(e): unauthorized use of any information technology system;

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;

AG ¶ 40(g): negligence or lax security practices in handling information technology that persists despite counseling by management; and

AG ¶ 40(h): any misuse of information technology, whether deliberate or negligent, that results in damage to the national security.

There is no evidence in the record establishing AG ¶ 40(a) through 40(f) and 40(h). AG ¶ 40(g) is partially established by Applicant's introduction of a personal CD-ROM into a secure workplace and his off-duty presence in a secure work area for personal convenience, but there is no evidence that he did so after being counseled by management.

SOR ¶ 2.b alleges that Applicant was terminated as a consequence of the conduct alleged in SOR ¶¶ 1.a-1.e, but it does not allege any additional conduct. The security significance of his termination is discussed below under Guideline E.

Guideline E, Personal Conduct

The SOR alleges that Applicant was terminated from employment because of the eight concerns in his former employer's August 2018 email. The security concern under this guideline is set out in AG ¶ 15: "Conduct involving questionable judgment, lack of candor, dishonesty, or unwillingness to comply with rules and regulations can raise questions about an individual's reliability, trustworthiness, and ability to protect classified or sensitive information. . . ."

The following disqualifying conditions under this guideline are relevant:

> 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; and
>
> 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 . . . (2) any disruptive, violent, or other inappropriate behavior; [or] (3) a pattern of dishonesty or rule violations.

AG ¶ 16(c) is not established. Applicant's minor security violations fall under Guidelines K and M, but when considered as a whole, they do not support a whole-person assessment of characteristics indicating that he may not properly safeguard classified or sensitive information.

AG ¶ 16(d) is partially established. Most of the conduct alleged and established by the evidence is explicitly covered by other guidelines. The evidence is insufficient to establish a pattern of rule violations. There is no evidence of aggressive or disruptive behavior covered by AG ¶ 16(d)(3). The evidence is sufficient to establish that Applicant took off his glasses and rubbed his head while a senior executive was speaking. As such, this conduct falls short of being aggressive. However, the evidence is sufficient to establish inappropriate behavior under AG ¶ 16(d)(2).

The following mitigating condition under this guideline is potentially applicable:

> 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.

This mitigating condition is established. Applicant's conduct was minor, infrequent, and happened more than four years ago.

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. An administrative judge should consider the nine adjudicative process factors listed at AG ¶ 2(d):

> (1) the nature, extent, and seriousness of the conduct; (2) the circumstances surrounding the conduct, to include knowledgeable participation; (3) the frequency and recency of the conduct; (4) the individual's age and maturity at the time of the conduct; (5) the extent to which participation is voluntary; (6) the presence or absence of rehabilitation and other permanent behavioral changes; (7) the motivation for the conduct; (8) the potential for pressure, coercion, exploitation, or duress; and (9) the likelihood of continuation or recurrence.

I have incorporated my comments under Guideline K, M, and E in my whole-person analysis and applied the adjudicative factors in AG ¶ 2(d).

After weighing the disqualifying and mitigating conditions under Guidelines K, M, and E, and evaluating all the evidence in the context of the whole person, I conclude that the evidence fails to establish the conduct alleged in SOR ¶¶ 1.a, 1.b, 1.c, and 2.a, and Applicant has mitigated the security concerns raised by his minor security violations alleged in SOR ¶¶ 1.d and 1.e and the inappropriate behavior and termination of employment alleged in SOR ¶ 3.a.

Formal Findings

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

Paragraph 1, Guideline K, (Handling Protected Information): FOR APPLICANT,

Subparagraphs 1.a-1.e: For Applicant

Paragraph 2, Guideline M (Use of Information Technology):	FOR APPLICANT
Subparagraphs 2.a and 2.b:	For Applicant
Paragraph 3, Guideline E (Personal Conduct):	FOR APPLICANT
Subparagraph 3.a:	For Applicant

Conclusion

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

LeRoy F. Foreman
Administrative Judge