DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 24-02486
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Cynthia Ruckno, Esq., Department Counsel
For Applicant: *Pro se*

12/11/2025

Decision

BORGSTROM, Eric H., Administrative Judge:

Applicant did not mitigate the use of information technology (IT) security concerns. Eligibility for access to classified information is denied.

Statement of the Case

On April 15, 2025, the Defense Counterintelligence and Security Agency (DCSA) issued a Statement of Reasons (SOR) to Applicant detailing a security concern under Guideline M (use of IT). The DCSA acted under Executive Order (EO) 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) implemented by the DOD on June 8, 2017.

In Applicant's April 23, 2025 response to the SOR (Answer), he admitted the single allegation. He acknowledged the impropriety and immaturity of his actions and explained that he was unaware of the severity of his misconduct. He did not attach any documentary evidence. He requested a decision by an administrative judge of the Defense Office of Hearings and Appeals based upon the written record in lieu of a hearing. (Answer)

On June 15, 2025, Department Counsel submitted a file of relevant material (FORM) and provided a complete copy to Applicant. Department Counsel's FORM included Government Exhibits (GE) 1 through 5. In the FORM, Department Counsel provided Applicant notice that failure to respond to the FORM may be considered a waiver of any objections to the admissibility of the evidentiary exhibits.

On June 23, 2025, Applicant received the FORM and its attachments. A cover letter included with the FORM advised Applicant that he had 30 days from the date of receipt to file any objections or to provide any additional information in support of his clearance eligibility. On June 25, 2025, he submitted a one-page response to the FORM and attached two character-reference letters, which I marked collectively as Applicant Exhibit (AE) A, and a performance review (AE B).

The case was assigned to me on September 30, 2025. GE 1 through 5, AE A, and B are admitted into evidence without objection. My decision was delayed when all administrative judges were furloughed from October 1 through November 12, 2025, during a federal government shutdown due to a lapse in federal funding.

Findings of Fact

Applicant is 48 years old. He graduated from high school in 1995 and earned a certificate of completion from a technical school in 2006. From November 1996 to November 1998, he served on active duty in the U.S. Army, and he was discharged under Other Than Honorable (OTH) conditions. From May 2016 to November 2023, he was employed as a senior technical analyst for a private company (Employer A). Since November 2023, he has been employed as a systems administrator with a DOD contractor. He has never married, and he has a 21-year-old child. (GE 3, GE 5)

On March 7, 2024, Applicant certified and submitted an Electronic Questionnaire for Investigations Processing (e-QIP). Under Section 22 – Police Record, he reported that he had been charged with larceny, a felony, in September 1998, after he cashed a check stolen from another soldier. He was discharged under OTH conditions in lieu of a courts martial proceeding. Under Section 25 – Investigations and Clearance Record, he reported that he had been granted a secret clearance in June 2009. Under Section 27 – Use of Technology Systems, he responded "NO" to the following query:

> In the last seven (7) years have you illegally or without authorization, modified, destroyed, or manipulated, or denied others access to information residing on an information technology system or attempted any of the above? (GE 3)

On April 25, 2024, Applicant was interviewed by an authorized investigator on behalf of the Office of Personnel Management (OPM). During the interview, he explained that, in about September 1998, he had cashed a check ($900) stolen from another soldier. He admitted that he had acted to get extra money. He was charged with larceny, a felony, and received an OTH discharge from the Army. (GE 4)

During the OPM interview, Applicant also admitted that, while employed with Employer A, he manipulated an IT system without authorization to change the password(s) of one or more employees[1]. He explained that he would act in such a manner when he felt angry towards or disrespected by the co-worker(s), who would then be unable to log into the IT system. The co-worker(s) would then need to seek Applicant's assistance, as a systems administrator, to regain access to the IT system. At the time, he was aware that using his administrator privileges to change passwords and deny access to an IT system was prohibited. Applicant was not caught engaging in this conduct. (GE 4)

In Applicant's February 21, 2025 response to DOHA interrogatories, he adopted the summary of the OPM interview without any corrections. He stated that he had changed the passwords of co-workers, without authorization, on approximately six occasions after they "raised voices, [made] condescending remarks or tone, insults." His actions were not discovered. "I joked about it with my team, and [I] was never formally reprimanded. I was discouraged from the behavior by team leaders." (GE 4)

Whole Person

Applicant proffered two character-reference letters from his current employment in support of his clearance eligibility. Applicant's team lead praised his "exceptional integrity and character," honesty, dependability, professionalism, and work ethic. A co-worker described him as "a dependable, honest, and highly capable individual," and she praised his work ethic, professionalism, and integrity. Neither reference indicated any awareness of the conduct raised in the SOR. (AE A)

The evidentiary record included five of Applicant's performance reviews from employment with Employer A. He received "satisfactory" and "commendable" ratings for each year reviewed. With his response to the FORM, Applicant included a favorable 2024 performance appraisal from his current employer. (GE 5; AE B)

Policies

When evaluating an applicant's suitability for a security clearance, the administrative judge must consider the adjudicative guidelines. In addition to brief introductory explanations for each guideline, the adjudicative guidelines list potentially disqualifying conditions and mitigating conditions, which are to be 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, administrative judges apply the guidelines 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(a),

[1] The record evidence does not specify whether Applicant's misconduct targeted one co-worker six times or six different co-workers.

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."

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

A person who seeks access to sensitive 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 sensitive information. Decisions include, by necessity, consideration of the possible risk the applicant may deliberately or inadvertently fail to safeguard sensitive information. Such decisions entail a certain degree of legally permissible extrapolation of potential, rather than actual, risk of compromise of sensitive information.

Section 7 of EO 10865 provides that adverse 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 M: Use of Information Technology

The security concern for use of IT 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 guideline notes several conditions that could raise security concerns under AG ¶ 40. The following disqualifying conditions are potentially applicable in this case:

> (b) unauthorized modification, destruction, or manipulation of, or denial of access to, an information technology system or any data in such a system; and
>
> (e) unauthorized use of any information technology system.

Applicant admitted that, on approximately six occasions during his employment with Employer A (May 2016 to November 2023), he deliberately accessed Employer A's IT system and changed the password for the accounts of one or more co-workers on that IT system. Without a functioning password, the individual was denied access to the IT system. The record evidence does not provide more specific information as to the type of IT system involved. At the time of his conduct, Applicant held administrator privileges for the IT system involved and was aware that his conduct was unauthorized and prohibited. He engaged in this conduct when he felt disrespected or mistreated by the co-worker(s) he targeted. AG ¶¶ 40(b) and 40(e) are established

Use of IT security concerns may be mitigated under AG ¶ 41. The following are potentially applicable in this case:

> (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;
>
> (b) the misuse was minor and done sole in the interest of organizational efficiency and effectiveness;
>
> (c) the conduct was unintentional or inadvertent and was followed by a prompt, good-faith effort to correct the situation and by notification to appropriate personnel; and
>
> (d) the misuse was due to improper or inadequate training or unclear instructions.

Applicant repeatedly and knowingly violated the trust placed in him as a system administrator to spitefully deny a co-worker access to Employer A's IT system. This misuse of IT systems was not due to improper or inadequate training or in furtherance of organizational efficiency or effectiveness. AG ¶¶ 41(b), 41(c), and 41(d) do not apply.

The revelation of Applicant's misconduct occurred when he disclosed this information during his April 2024 OPM interview; however, this information should have been reported under Section 27 of his March 2024 e-QIP. Applicant was employed by Employer A from May 2016 to November 2023, but the record evidence does not provide more specific information as to when the misconduct occurred. Applicant was between

the age of 38 and 45 at the time of his misconduct. The catalyst for Applicant's misconduct was his perceived insult or mistreatment by a co-worker while he held administrator privileges. There is no evidence that anyone with Applicant's current employer is aware of his misconduct. Applicant has not identified any "unusual circumstances" which triggered his misconduct which would now make that conduct unlikely to recur. While there is no evidence of any harm – besides inconvenience or delay, caused to Applicant's co-workers – Applicant has not provided sufficient evidence in mitigation to establish that the circumstances and prohibited behavior are mitigated by the passage of time and unlikely to recur. AG ¶ 41(a) does not apply. Applicant did not mitigate the use of IT systems security concerns.

Whole-Person Concept

Under the whole-person concept, the administrative judge must evaluate an applicant's eligibility for access to classified information by considering the totality of the applicant's conduct and all relevant 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 Guideline M and the factors in AG ¶ 2(d) in this whole-person analysis.

Applicant received favorable performance reviews from Employer A and his current employer. His team lead and co-worker praised his exceptional integrity, honesty, dependability, professionalism, and work ethic; however, neither reference indicated any awareness of the conduct raised in the SOR. While Applicant's conduct may have seemed immature and less serious to him, he repeatedly and knowingly violated the trusted placed upon him as a systems administrator when he denied co-workers access to Employer A's IT system. This conduct occurred when he was in professional environment and at least 38 years old, and the record evidence does not establish that his misconduct is unlikely to recur.

Because Applicant elected a decision based upon the written record instead of a hearing, I did not have the opportunity to observe his testimony and assess his credibility

in that context. Applicant's misconduct, while holding a position of responsibility and access as a systems administrator, does not reflect the responsibility and good judgment of one entrusted to safeguard sensitive and classified information. This decision should not be construed as a determination that Applicant cannot obtain a security clearance in the future. Eligibility for access to classified information is denied.

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 M:	AGAINST APPLICANT
Subparagraph 1.a.:	Against Applicant

Conclusion

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

Eric H. Borgstrom
Administrative Judge