DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 24-01592
	)	
	)	
Applicant for Security Clearance	)	

Appearances

For Government: John Renehan, Esq., Department Counsel
For Applicant: *Pro se*

02/10/2026

Decision

LOKEY ANDERSON, Darlene D., Administrative Judge:

Statement of Case

On January 31, 2024, Applicant submitted a security clearance application (e-QIP). On January 30, 2025, the Defense Counterintelligence and Security Agency Consolidated Adjudication Services (DCAS CAS) issued Applicant a Statement of Reasons (SOR), detailing security concerns under Guideline K, Handling Protected Information; Guideline M, Use of Information Technology; and Guideline E, Personal Conduct. The action was taken under Executive Order (EO) 10865, *Safeguarding Classified Information within Industry* (February 20, 1960), as amended; Department of Defense Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (January 2, 1992), as amended (Directive); and the *National Security Adjudicative Guidelines for Determining Eligibility for Access to Classified Information or Eligibility to Hold a Sensitive Position* (AG), effective within the DoD after June 8, 2017.

Applicant answered the SOR on March 18, 2025, and requested a hearing before an administrative judge. The case was assigned to me on July 14, 2025. The Defense Office of Hearings and Appeals issued a notice of hearing on November 18, 2025, and the hearing was convened as scheduled on January 6, 2026. The Government offered two exhibits, referred to as Government Exhibits 1 and 2, which were admitted without objection. Applicant offered no exhibits, but he did testify on his own behalf. The record remained open until close of business on January 13, 2026, to allow the Applicant the opportunity to submit supporting documentary evidence. Applicant submitted an index and six documents, collectively referred to as Applicant's Post-Hearing Exhibit A which was admitted into evidence. DOHA received the final transcript of the hearing (Tr.) on January 15, 2026. This 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 41 years old. He is not married and has no children. He has a high school diploma and some college, equivalent to an Associate degree. He is applying for a position as a background investigator for a defense contractor. A security clearance is necessary in connection with his employment. Applicant has no miliary service.

Guideline K – Handling Protected Information

The Government alleged that Applicant is ineligible for a clearance because he deliberately or negligently failed to comply with rules and regulations for handling protected information; which includes classified and other sensitive government information and proprietary information, and raises doubt about his trustworthiness, judgment, reliability, or willingness and ability to safeguard such information.

Guideline M – Use of Information Technology

The Government alleged that Applicant is ineligible for a clearance because he failed to comply with rules, procedures, guidelines, or regulations pertaining to information technology systems; which raise security concerns about his reliability and trustworthiness, calling into question his 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.

In 2012, Applicant first applied for a Highway Patrol position as a cadet. He went into the academy, but failed during vehicle maneuver training. He applied a second time in 2014, and went into the academy again. Again, he failed the vehicle maneuver training. He then decided to take private EVOC (which is high-speed vehicle maneuvering). After a third time attempt, Applicant passed the vehicle maneuver training for the Highway Patrol. He graduated from the academy in January 2016, and became an official duty-bound officer with the State Highway Patrol. He was employed there until November 2022. (Tr. pp. 16-18.)

As a Highway Patrol Officer, Applicant had access to the State Law Enforcement Agency Telecommunications system, which is known as the CLETS system. This is a computer database that has access to all DMV records and the driving history of individuals who have applied for or possess a valid driver's license and vehicle registration in the state. It also maintains records concerning violations of the vehicle code, including DUI arrests, and other related citations, such as speeding, reckless driving, etc. (Tr. pp. 23-24.) There are two ways to access the CLETS system. One is through a highway patrol vehicle where the system is installed, the other is through the internal computer located at their office. Applicant was trained on the CLETS system before becoming an officer. He stated that he had to pass a course at the end of each training session to ensure that he understood that he was only allowed to use the CLETS system on a need-to-know or right-to-know basis. This meant that if he was working on a case that required this information, he was able to access it; or if he had authority to access it based upon a work-related matter, he could access it. Nothing else. (Tr. p. 25.) He was permitted to use the system only in the course of his duties, for example if he pulled someone over and needed to check their DMV record. (Tr. p. 25.) He also received training on handling protected, private or confidential information that might be in CLETS. He stated that he was also instructed never to leave the system on, and never to show anyone how to access the system. All information he prints out from the CLETS must be destroyed, and is not for the general public. (Tr. p. 25)

In April 2020 an associate from high school, who Applicant kept in touch with through mutual friends, contacted Applicant and asked him for a favor. He asked Applicant if he would run a car's license plate for him claiming it was linked to his stolen property. Applicant agreed to do it, and he used the CLETS system to obtain the information for this associate. Applicant then texted the vehicle record to this associate. Unknown to the Applicant, this associate was under surveillance by the FBI for unknown criminal activities, and Applicant's text message was discovered during their investigation. Applicant later found out that this associate was associated with a criminal gang. During the highway patrol internal investigation, it was revealed that this associate intended to use the vehicle information to kill the owner of the vehicle. (Government Exhibit 2.)

During the investigation, Applicant was asked if he had accessed the CLETS system other times not related to his official duties. He admitted that he had used the system on two other occasions for friends who were applying to the highway patrol academy. He stated that he checked their records for any adverse information. He stated that he did not release any confidential information. Applicant also stated that he ran numerous record checks on his own name to determine if the system was working that particular day. He stated that he has on occasion had difficulties with it working properly. It was ultimately discovered that Applicant accessed the system a total of 29 times not related to his work.

Applicant served as an Highway Patrol Officer from 2016 through 2022. As a result of the information discovered by the FBI and then the Highway Patrol during their investigations, Applicant resigned in lieu of being terminated. He is not eligible of rehire.

Guideline E – Personal Conduct

The Government alleges that Applicant is ineligible for a clearance because he engaged in conduct involving questionable judgment, lack of candor, dishonesty, or unwillingness to comply with rules and regulations which raises questions about his 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.

Applicant knowingly violated department policy by intentionally accessing the State Law Enforcement System on numerous occasions, not related to his official duties. He also deliberately texted protected information that he accessed from CLETS to an unauthorized individual. Applicant's misconduct shows poor judgment, unreliability, and untrustworthiness.

Applicant stated that he takes full responsibility for his actions, he regrets what he did, and realizes that he made a stupid mistake that could have been very dangerous. He stated that he did not know that his associate was a part of any criminal activities. He stated that he has learned from his mistake.

During his tenure as a Highway Patrol Officer, Applicant received multiple awards and recognition for valor, specifically for saving lives while on duty. These awards include, The Governor's Medal of Valor, with a Certificate and letter from 2021; A Special Act Award (Gold) 2017; a Certificate of Commendation for Exceptional Performance 2019; an Officer of the Year Award; Two Crime Stoppers Awards, 2018 and 2019; and various letters of appreciation from public and private organizations. (Applicant's Post-Hearing Exhibit A.)

Policies

When evaluating an applicant's suitability for national security eligibility, the administrative judge must consider the adjudicative guidelines (AG). 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 AG ¶ 2 describing the adjudicative process. The administrative judge's overarching adjudicative goal is a fair, impartial, and commonsense decision. 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. 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 clearance 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 the 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 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 K - Handling Protected Information

The security concern relating to the guideline 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.

The guideline notes several conditions that could raise security concerns under AG ¶ 34. Three are potentially applicable in this case:

> (d) inappropriate efforts to obtain or view protected information outside one's need to know;
>
> (f) viewing or downloading information from a secure system when the information is beyond the individual's need to know; and
>
> (g) any failure to comply with rules for the protection of classified or sensitive information.

Applicant knowingly violated department policy when he accessed and texted protected information from the CLETS system. The evidence is sufficient to raise the above disqualifying conditions.

AG ¶ 35 provides conditions that could mitigate security concerns. I considered all of the mitigating conditions under AG ¶ 35 including:

> (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.

Applicant was deliberate and negligent when he knowingly violated department policy and accessed the CLETS system. His misconduct occurred recently, just 4 years ago, and was egregious and reckless. None of the mitigating conditions are applicable. His conduct casts doubt on Applicant's current reliability, trustworthiness, and good judgment.

Guideline M - Use of Information Technology

The security concern relating to the guideline for Use of information Technology 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 and calls into question the willingness or ability to property protect sensitive systems, networks, and information.

The guideline notes several conditions that could raise security concerns under AG ¶ 40. Two are potentially applicable in this case:

(a) unauthorized entry into any information technology system; and

(e) unauthorized use of any information technology system.

AG ¶ 41 provides conditions that could mitigate security concerns. I considered all of the mitigating conditions under AG ¶ 41 including:

(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 solely 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 failed to follow rules, procedures, guidelines, or regulations, concerning the use of the CLETS system. He knowingly violated department policy just four years ago, which is fairly recent. He did not report this misconduct to his superiors, in fact it was only discovered during an FBI investigation, and then followed up by his department's internal investigation. He had received proper training on the CLETS system, and had taken the tests after each section of the training to ensure that he understood the rules. There is no excuse for his misconduct. None of the mitigating conditions are applicable.

Guideline E - Personal Conduct

The security concern relating to the guideline for Personal Conduct 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.

The guideline notes several conditions that could raise security concerns under AG ¶ 16. Three are potentially applicable in this case:

(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;

(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:

(1) untrustworthy or unreliable behavior to include breach of client confidentiality, release of proprietary information, unauthorized release of sensitive corporate or government protected information;

(2) any disruptive, violent, or other inappropriate behavior;

(3) a pattern of dishonesty or rule violations;

(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

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

After extensive training as a Highway Patrol Officer, over a six-year period, Applicant knowingly violated department policy by intentionally accessing the CLETS systems on 29 occasions not related to his official duties. The evidence is sufficient to raise the above disqualifying conditions.

AG ¶ 17 provides conditions that could mitigate security concerns. I considered all of the mitigating conditions under AG ¶ 17 including:

(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;

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

(f) the information was unsubstantiated or from a source of questionable reliability.

Applicant's misconduct is very troubling. As a Highway Patrol Officer, he had extensive training on the CLETS system, and knew that the way he was using it was clearly prohibited. He violated department policy without thought or consideration for serious ramifications or dangerous consequences that could result. Applicant was immature and big-headed. His judgment is questionable and indicative of unreliability, and untrustworthiness. Insufficient mitigation has been shown. None of the mitigating conditions are applicable.

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 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 relevant facts and circumstances surrounding this case. With a position requiring a security clearance, the Government must be able to trust the individual to do the right thing in every circumstance, even when no one is looking. Applicant falls short of meeting this requirement. Applicant knowingly violated department policy by intentionally accessing the CLETS systems on numerous occasions not related to his official duties. On at least one occasion he even texted private records from the CLETS system to an unauthorized individual. The individual happened to be a criminal. No one was looking at Applicant's conduct until the FBI discovered it during their investigation. Then and only then was it determined that Applicant had been violating highway patrol policy for several years. His misconduct demonstrates immaturity, poor judgment, unreliability, and untrustworthiness. He has failed to meet his burden of proving that it is clearly consistent with the national interests to grant his clearance. Accordingly, I conclude Applicant has not mitigated the Handling of Protected Information, the Use of Information Technology, and Personal Conduct security concerns.

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

Conclusion

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

Darlene Lokey Anderson
Administrative Judge