OFFICIAL PUBLICATION OF GCIS

SERVICE SECURITY CLEARANCE PROGRAM

RELEASED
JUNE 09, 2026

VERSION: **SC-1.210**

CLASSIFIED

[redacted]

Approved by the Office of the Director

GCIS Security Clearance Overview

The Ground Coordination Intelligence Service (GCIS) maintains a tiered security clearance system designed to protect sensitive information, operational capabilities, personnel identities, intelligence sources, investigative activities, and organizational interests from unauthorized access, disclosure, compromise, or misuse. The security clearance program serves as a foundational component of GCIS's broader information security, operational security (OPSEC), compartmentation, and risk management framework.

The primary purpose of the clearance system is to ensure that members are granted access only to the information, systems, facilities, operations, and resources necessary to perform their authorized duties. Access to protected information is based upon a combination of trust, demonstrated reliability, operational necessity, and mission requirements. Security clearances are therefore issued not as a privilege of rank, position, tenure, or organizational status, but as a carefully controlled authorization intended to safeguard the integrity of GCIS operations and the safety of personnel, victims, witnesses, sources, and partner organizations.

Possession of a security clearance alone does not entitle an individual to unrestricted access to information. All information within GCIS remains subject to the principles of compartmentation and need-to-know. Personnel must possess both the appropriate clearance level and a legitimate operational, investigative, administrative, supervisory, or support-related requirement for access before information may be disclosed. Access determinations may be restricted, modified, suspended, or revoked at any time based upon operational requirements, security considerations, or changes in assignment and require no justification by GCIS.

GCIS utilizes a layered approach to information protection whereby increasingly sensitive information is protected through progressively higher clearance levels and compartmented access controls. Certain information may be restricted to specific directorates, operational groups, intelligence components, task forces, or mission elements regardless of an individual's overall clearance level. As a result, personnel may possess a clearance level that exceeds the classification of information required for their current assignment while still being prohibited from accessing information outside their authorized mission scope.

Particularly sensitive intelligence, [redacted], source-identifying information, cover identities, and compartmented mission data are subject to enhanced access restrictions beyond standard clearance requirements. Access to such information is granted only to specifically authorized personnel who have undergone additional vetting, indoctrination, and approval processes and who maintain a demonstrated need-to-know directly related to their assigned duties.

All personnel granted a GCIS security clearance assume a continuing obligation to protect protected information from unauthorized disclosure, compromise, loss, theft, misuse, or exploitation. These responsibilities remain in effect throughout an individual's affiliation with GCIS and continue after resignation, retirement, reassignment, contract termination, or any other separation from service. Failure to comply with clearance requirements, security procedures, compartmentation rules, or confidentiality obligations may result in administrative action, suspension or revocation of access privileges, disciplinary measures, termination of affiliation, civil liability, criminal referral, or other lawful remedies deemed appropriate by GCIS authorities and criminal courts as directed.

The GCIS Security Clearance Program is therefore intended not only to regulate access to information, but also to reinforce a culture of accountability, discretion, professionalism, and operational security throughout the service. Every cleared individual serves as a steward of the information entrusted to them and bears personal responsibility for ensuring that such information remains protected in accordance with GCIS policies, directives, and security requirements as well as U.S. Code as directed and applicable.

GENERAL CLEARANCE (G)

The General Clearance represents the entry-level security authorization within the Ground Coordination Intelligence Service (GCIS) and is intended for individuals whose duties require limited access to GCIS facilities, personnel, resources, or support functions but who do not require routine access to sensitive operational, investigative, intelligence, or compartmented information. This clearance level exists to ensure that personnel who provide essential support services to the service can perform their duties while maintaining appropriate safeguards for protected information and operational security. General Clearance holders typically include facility maintenance personnel, custodial staff, contracted support personnel, authorized third-party service providers, vendors, temporary support staff, and certain government, humanitarian, or non-governmental organization representatives who may periodically interact with GCIS members or facilities in an authorized capacity or non-restricted area (accept when authorized by the Office of the Director).

Eligibility for a General Clearance is based upon an individual's demonstrated trustworthiness, reliability, and suitability to operate within a security-conscious environment. Applicants must be at least eighteen years of age and successfully complete identity verification procedures to establish and confirm their legal identity. Prospective clearance holders are subject to a criminal history review designed to identify conduct that may present a security risk or raise concerns regarding their ability to safeguard protected information. Individuals seeking General Clearance access must execute the official GCIS Non-Disclosure Agreement and acknowledge their ongoing obligation to protect confidential information encountered during the course of their duties. Applicants are also required to complete introductory Operational Security (OPSEC) awareness training and cybersecurity awareness training to ensure a basic understanding of security responsibilities, information handling requirements, reporting obligations, and common threats to organizational security. Additionally, applicants must demonstrate no known affiliation with criminal enterprises, extremist organizations, hostile actors, or any individual or group whose interests may conflict with the mission, members, or strategic interests of GCIS.

Prior to the issuance of a General Clearance, applicants are required to provide specific documentation to support the vetting process. At a minimum, this documentation includes government-issued identification, a completed background information questionnaire, proof of employment or contractual relationship with GCIS or an authorized partner organization, emergency contact information, and a signed copy of the GCIS Non-Disclosure Agreement. The review of these materials allows investigators from the Bureau of Professional standards to establish an accurate record of the individual's identity, employment status, and suitability for access to GCIS-controlled facilities and environments. General Clearances are not considered permanent authorizations and remain subject to periodic review. On an annual basis, clearance holders are required to reaffirm their confidentiality obligations under the NDA, complete security awareness refresher training, undergo a review of their credentials and access privileges, and provide updated contact or employment information as necessary. These recurring requirements help ensure that personnel remain aware of current security expectations and continue to meet eligibility standards throughout the duration of their access.

Personnel holding a General Clearance may be authorized to enter designated non-sensitive work areas, administrative support spaces, logistical support environments, and other locations specifically approved for their duties. They may also participate in authorized support activities that assist GCIS operations without requiring exposure to protected operational information. However, General Clearance holders are expressly prohibited from accessing intelligence products, operational plans, investigative records, source-identifying information, victim or witness information, compartmented systems, restricted databases, sensitive communications, or any information whose disclosure could adversely affect operations, personnel, sources, or organizational interests. Access granted under a General Clearance is further governed by the principles of need-to-know and least privilege, meaning that personnel may only access the specific facilities, systems, and information necessary to perform their assigned responsibilities.

Although General Clearance holders are not entrusted with the same degree of sensitive information as personnel holding Secret, Top Secret, or TS/SCI clearances, they remain subject to all applicable security, confidentiality, and reporting

requirements established by GCIS policy. Any unauthorized access, disclosure, retention, transmission, misuse, or compromise of protected information may constitute a security violation and result in immediate corrective action. Depending on the nature and severity of the violation, consequences may include immediate removal from GCIS facilities, suspension or revocation of credentials and access privileges, termination of employment or contractual relationships, administrative investigations, civil liability, and referral to law enforcement authorities for criminal investigation when warranted. General Clearance holders are therefore expected to exercise professionalism, discretion, and sound judgment at all times while performing duties on behalf of or in support of GCIS operations.

SECRET CLEARANCE (S)

The Secret Clearance serves as the foundational operational security clearance within the Ground Coordination Intelligence Service (GCIS) and is held by the majority of members actively engaged in organizational activities. Unlike General Clearance holders, Secret-cleared members routinely encounter protected information, sensitive records, operational support materials, service data, and internal organizational information that, if improperly disclosed, could adversely affect investigations, operational effectiveness, operators and asset safety, victim privacy, source protection, or the overall mission of GCIS. The Secret Clearance is intended to provide authorized members with the level of access necessary to perform investigative, administrative, analytical, technical, logistical, and support-related duties while maintaining appropriate safeguards for sensitive information and organizational resources.

Members typically assigned a Secret Clearance include administrative personnel, dispatch personnel, intelligence and operational analysts, technical specialists, information technology personnel, cybersecurity personnel, logistics staff, non-criminal investigators, operational support specialists, records management specialists, training staff (non-CAG/ICS), communications specialists, and other individuals whose duties require regular interaction with protected information but do not necessitate access to highly compartmented or exceptionally sensitive intelligence holdings. The Secret Clearance represents a position of significant trust and requires members to demonstrate an elevated level of professionalism, discretion, and accountability in the performance of their duties.

Eligibility for a Secret Clearance begins with satisfaction of all requirements associated with the General Clearance program and expands upon those standards through a more comprehensive suitability assessment. Applicants must successfully complete a formal background investigation designed to evaluate their character, reliability, integrity, judgment, and ability to safeguard protected information. The investigation may include verification of identity, employment history, educational records, professional qualifications, residential history, criminal records, and references capable of attesting to the applicant's trustworthiness and suitability for access to sensitive information. Applicants must demonstrate a consistent history of responsible conduct, sound decision-making, and adherence to ethical and professional standards. Particular attention may be given to any history of dishonesty, unauthorized disclosures, misuse of information systems, criminal activity, financial irresponsibility, or conduct that could create vulnerabilities to coercion, exploitation, manipulation, or compromise.

Prospective Secret Clearance holders are required to complete formal Operational Security (OPSEC) training, cybersecurity awareness training, information handling instruction, confidentiality training, and any additional security education prescribed by GCIS BPS/DOI/DSM/OD. Applicants must demonstrate an understanding of the principles of compartmentation, need-to-know access, information classification, source protection, victim protection, digital security, reporting requirements, and operational confidentiality. Because Secret-cleared members frequently serve as custodians of sensitive information, they must also demonstrate the ability to exercise sound judgment when handling protected records, responding to information requests, utilizing organizational systems, and interacting with other members, partners, and external organizations.

Prior to adjudication, applicants are generally required to submit a comprehensive personnel history statement detailing relevant personal, educational, employment, military, volunteer, and residential information. Supporting documentation may include employment history covering at least the previous seven years, professional references, criminal history disclosures, financial responsibility information, and any additional records deemed necessary to evaluate suitability. Applicants must execute the GCIS Non-Disclosure Agreement and participate in a formal security interview conducted by authorized personnel. During the security interview, applicants may be questioned regarding prior conduct, foreign travel, foreign associations, financial circumstances, cybersecurity practices, professional history, and other matters relevant to determining their suitability for access to protected information.

Secret Clearances remain subject to continuous review throughout the holder's affiliation with GCIS. At a minimum, personnel are required to participate in annual security review interviews and access validation reviews to ensure that continued access remains operationally necessary and security concerns have not emerged. Personnel must complete recurring OPSEC and cybersecurity training, maintain familiarity with current security directives, and promptly disclose information that may affect their eligibility for continued access. Annual reporting requirements may include disclosure of foreign contacts, foreign travel, arrests, criminal charges, civil judgments, significant financial difficulties, security incidents, credential compromises, cybersecurity events, or other matters that could potentially affect trustworthiness, reliability, or operational suitability.

Secret-cleared members may be granted access to a broad range of protected information necessary to support GCIS operations. Such access may include standard operating procedures, internal policies, personnel records, victim information, witness information, operational support documentation, internal communications, investigative support materials, training resources, administrative security information, technical documentation, and other protected organizational records. However, possession of a Secret Clearance does not grant unrestricted access to all information maintained by GCIS. All access remains governed by the principles of need-to-know, least privilege, and compartmentation. Personnel are authorized to access only the information required to perform their assigned duties, regardless of their clearance level, position, or organizational seniority. Access may be restricted, suspended, modified, or revoked whenever operational requirements, security concerns, or mission priorities warrant such action.

Secret-cleared members assume substantial responsibilities regarding the protection of information and organizational resources. They are expected to maintain strict confidentiality concerning operational activities, personnel information, victim data, witness information, investigative matters, source-related information, security procedures, communications systems, and other protected information. Personnel shall utilize only authorized systems and communications channels when accessing, processing, transmitting, or storing protected information and shall comply with all applicable digital security requirements, credential management procedures, and information handling standards. Secret-cleared personnel are further required to report actual or suspected security incidents, unauthorized disclosures, suspicious inquiries, cybersecurity events, credential compromises, or any other circumstance that may threaten organizational security.

Certain conduct is expressly prohibited for Secret Clearance holders due to the risks such behavior poses to operational security and organizational integrity. Personnel shall not discuss protected information outside authorized channels, disclose information to individuals lacking a legitimate need-to-know, store protected information on personal devices or unauthorized systems, share credentials or authentication mechanisms, access records unrelated to their official duties, circumvent security controls, remove protected information from authorized environments without approval, or publicly discuss investigations, operations, personnel, capabilities, or organizational activities. These prohibitions are reinforced throughout GCIS policy and the Non-Disclosure Agreement, particularly within provisions governing operational security, digital security, social media usage, credential protection, source protection, victim protection, and compartmented information controls.

Violations involving Secret-cleared members are treated seriously due to the sensitivity of the information entrusted to them. Depending upon the nature and severity of the violation, consequences may include temporary suspension of access privileges, formal security investigations, administrative discipline, mandatory retraining, reassignment, removal from operational duties, clearance suspension, clearance revocation, termination of employment or affiliation, civil liability, and referral to law enforcement authorities for criminal investigation when appropriate. Deliberate misuse of protected information, unauthorized disclosure of sensitive records, compromise of victims or sources, misuse of organizational systems, or repeated violations of security requirements may result in permanent loss of clearance eligibility and exclusion from future access to GCIS protected information.

The Secret Clearance therefore serves as the cornerstone of the GCIS personnel security program, enabling trusted personnel to carry out essential operational, investigative, analytical, and support functions while ensuring that sensitive information remains protected from unauthorized disclosure, compromise, or exploitation. Holders of this clearance are entrusted with significant responsibilities and are expected to uphold the highest standards of professionalism, discretion, integrity, and security awareness throughout their service with GCIS.

TOP SECRET CLEARANCE (TS)

The Top Secret Clearance represents a senior-level security authorization within the Ground Coordination Intelligence Service (GCIS) and is reserved for personnel whose duties involve direct participation in highly sensitive operational, investigative, intelligence, cyber, and strategic mission activities. Individuals granted a Top Secret Clearance routinely encounter information whose unauthorized disclosure could result in severe operational compromise, jeopardize ongoing investigations, expose protected personnel or sources, damage international partnerships, undermine organizational capabilities, or create significant legal, security, financial, or personal consequences for affected individuals and operations. Due to the sensitivity of the information entrusted to these personnel, Top Secret Clearance holders are subject to enhanced vetting, heightened oversight, and increased accountability throughout the duration of their service.

Personnel typically assigned a Top Secret Clearance include Strategic Mission operators, cyber interdiction personnel, rescue and recovery operators, case officers, operational commanders, mission supervisors, senior intelligence analysts, mission planners, operational coordinators, specialized investigators, protective operations personnel, and other individuals whose duties require access to highly sensitive operational information. These personnel frequently participate in the planning, coordination, execution, oversight, or support of operations that involve elevated levels of risk, complexity, and sensitivity. Their responsibilities often place them in possession of information concerning active investigations, operational deployments, source activities, intelligence collection efforts, strategic organizational initiatives, specialized methodologies, and sensitive personnel matters that require protection beyond the level afforded by a standard Secret Clearance.

Eligibility for a Top Secret Clearance requires an applicant to meet all standards associated with the Secret Clearance program while also demonstrating an exceptional degree of trustworthiness, integrity, discretion, and professional maturity. Applicants must successfully complete an advanced background investigation designed to evaluate not only their personal reliability but also their ability to responsibly manage information that could cause significant harm if compromised. Security officials conducting the investigation may review employment history, residential history, financial records, professional conduct, prior security-related incidents, foreign travel, foreign contacts, legal matters, social media activity, digital presence, and other factors relevant to determining overall suitability for access to highly sensitive information. Because Top Secret personnel are frequently entrusted with information affecting ongoing operations and organizational security, particular attention is paid to identifying vulnerabilities that could expose an individual to coercion, manipulation, blackmail, exploitation, or other forms of compromise.

Applicants are further required to participate in a comprehensive security interview conducted by senior security personnel or designated adjudicators. During this process, applicants may be questioned regarding their professional history, decision-making abilities, handling of sensitive information, foreign associations, financial circumstances, prior disciplinary actions, cybersecurity practices, and any other matters deemed relevant to the adjudication process. In addition to satisfying investigative requirements, applicants must demonstrate operational maturity and possess a documented need for access based upon their assigned duties, operational responsibilities, or organizational role. A Top Secret Clearance is granted only when security authorities determine that access is both necessary and consistent with the security interests of GCIS.

The documentation required for initial adjudication is significantly more comprehensive than that required for lower clearance levels. Applicants must complete an expanded background investigation package and submit a detailed personal history statement addressing employment, education, military service, volunteer activities, residences, travel, legal matters, financial history, and professional affiliations. Security personnel may conduct multiple reference interviews and obtain supervisor endorsements to assess the applicant's character, professionalism, reliability, and operational judgment. Once investigative activities have concluded, the applicant's file undergoes a formal security adjudication review and operational suitability assessment to determine whether access should be granted. Final approval may require concurrence from designated security officials, command personnel, or organizational leadership depending upon the position involved.

Top Secret Clearance holders remain subject to continuous evaluation and periodic review throughout their affiliation with GCIS. At a minimum, personnel are required to participate in annual security reinvestigation interviews, clearance validation reviews, operational conduct assessments, and digital security compliance reviews. These reviews are intended to identify emerging risks, ensure continued operational suitability, and confirm that access remains necessary for assigned duties. Personnel must also comply with recurring reporting requirements regarding foreign contacts, foreign travel, arrests, criminal charges, civil litigation, significant financial issues, security incidents, credential compromises, cybersecurity events, or other matters that could affect eligibility. Although not always mandatory, periodic psychological wellness reviews are strongly encouraged due to the unique pressures associated with highly sensitive operational assignments and the nature of the information routinely encountered by Top Secret personnel.

In addition to annual reviews, all Top Secret Clearance holders are subject to a comprehensive reinvestigation at least every five years, or more frequently if circumstances warrant. These reinvestigations may include updated background inquiries, additional interviews, expanded record reviews, renewed adjudication assessments, and evaluations of operational performance. The purpose of the reinvestigation process is to ensure that personnel continue to meet the elevated standards required for access to highly sensitive information and operational activities.

Personnel holding a Top Secret Clearance may be authorized access to a wide range of highly sensitive information necessary to support strategic operations and organizational objectives. Such information may include active operational planning materials, deployment schedules, mission directives, sensitive investigative information, cyber operations data, strategic mission records, advanced operational capabilities, high-risk source information, intelligence collection activities, specialized methodologies, operational assessments, command-level communications, and information concerning ongoing or planned operations. Access to such information enables personnel to effectively perform critical functions within the organization while ensuring that sensitive activities remain protected from unauthorized disclosure or compromise.

However, possession of a **Top Secret Clearance does not constitute unrestricted access to all GCIS information.** Access remains governed by the principles of need-to-know, compartmentation, and mission necessity. Personnel are granted access only to the information required to perform their authorized duties, regardless of their rank, seniority, position, or clearance level. Furthermore, possession of a Top Secret Clearance does not automatically authorize access

to information protected under TS/SCI compartments. Such compartmented information requires separate authorization, additional vetting, and specific operational justification before access may be granted.

Because of the exceptionally sensitive nature of the information entrusted to them, **Top Secret Clearance holders are expected to maintain enhanced security practices at all times.** Personnel must immediately report actual or suspected security incidents, unauthorized disclosures, suspicious inquiries, cybersecurity compromises, foreign influence concerns, credential losses, and any other event that may affect organizational security. They are required to exercise heightened operational security awareness in both professional and personal environments and must take proactive measures to safeguard operational methodologies, investigative techniques, intelligence capabilities, source information, victim information, witness information, communications systems, and protected organizational activities. Secure communications practices, strict adherence to compartmentation requirements, and rigorous information-handling procedures are considered fundamental responsibilities of all Top Secret personnel.

Violations involving Top Secret information are regarded as among the most serious breaches of organizational security due to the potential consequences associated with compromise. Unauthorized disclosure of protected operational information may place personnel, sources, victims, witnesses, investigations, and ongoing operations at significant risk. Depending upon the severity of the violation, consequences may include immediate suspension of access privileges, emergency security debriefings, removal from operational assignments, reassignment pending investigation, clearance suspension or revocation, internal affairs investigations, administrative discipline, termination of employment or affiliation, civil litigation, and referral for criminal prosecution where applicable. Deliberate compromise of protected information, repeated security violations, unauthorized disclosure of source information, operational negligence, or conduct demonstrating an inability to safeguard sensitive information may result in permanent revocation of clearance eligibility and exclusion from future access to GCIS protected information.

The Top Secret Clearance therefore represents one of the highest levels of trust that can be granted within GCIS. Personnel entrusted with this clearance serve in positions that directly influence the success, safety, and effectiveness of the organization's most sensitive operations. As such, they are expected to exemplify the highest standards of professionalism, judgment, discretion, accountability, and commitment to operational security throughout their service and beyond.

TOP SECRET/ SENSITIVE COMPARTIMENTALIZED INFORMATION (TS/SCI)

The Top Secret / Sensitive Compartmented Information (TS/SCI) clearance represents the highest level of security authorization within the Ground Coordination Intelligence Service (GCIS). This clearance is reserved exclusively for a select group of individuals whose duties require access to the organization's most sensitive operational, intelligence, [redacted]. Individuals entrusted with TS/SCI access occupy positions of extraordinary trust and responsibility and serve as custodians of information whose unauthorized disclosure could result in catastrophic operational consequences, compromise active or future [redacted], expose protected individuals and intelligence assets, damage partnerships, reveal specialized capabilities, or place human lives at risk.

Unlike lower clearance levels, TS/SCI access is not granted solely on the basis of organizational position, seniority, or assignment to a particular directorate. Rather, access is provided only when an individual demonstrates both exceptional suitability and a verified operational necessity to participate in specifically designated compartmented programs, operations, investigations, intelligence activities, or mission elements. Individuals granted TS/SCI access are typically assigned to highly sensitive operational components within the Directorate of Strategic Missions and the Directorate of Intelligence, this includes groups like the [redacted], the [redacted], or other specially authorized compartmented programs established by the [redacted].

[redacted].

Eligibility for TS/SCI access begins with qualification for a Top Secret Clearance and requires an extensive additional review process focused on the applicant's ability to responsibly manage compartmented information. [redacted].

Particular emphasis is placed upon identifying vulnerabilities that could compromise compartmented information. Because TS/SCI personnel often possess information of extraordinary sensitivity, security authorities carefully assess any factors that may create susceptibility to coercion, exploitation, foreign influence, manipulation, blackmail, operational compromise, or unauthorized disclosure. Applicants may be required to participate in specialized counterintelligence interviews, security reviews, and compartment-specific suitability assessments designed to evaluate their ability to safeguard highly restricted information under complex operational conditions.

Personnel seeking TS/SCI access must complete [redacted]

[redacted].

[redacted]

[redacted]

[redacted]

[redacted].

Possession of TS/SCI access does not grant unrestricted access to all compartmented information maintained by GCIS. Compartmentation remains the fundamental principle governing TS/SCI operations. Personnel may only access the specific compartments for which they have received authorization, indoctrination, and documented operational need. Access to one compartment does not authorize access to any other compartment, regardless of the individual's clearance level, position, rank, or organizational authority. Information maintained within separate compartments remains segregated unless formal authorization is granted for limited sharing or integration.

Accordingly, TS/SCI personnel are prohibited from disclosing information across compartment boundaries without express authorization from the designated approving authority. They may not aggregate, correlate, analyze, compile, or merge information from multiple compartments unless specifically authorized in writing. Personnel are likewise prohibited from revealing the existence of protected compartments, acknowledging compartmented affiliations, confirming participation in [redacted], discussing compartmented operations outside authorized environments, or disclosing information

that could permit another individual to infer the existence of a protected program, source, capability, partnership, or mission. These restrictions apply regardless of whether the disclosure is direct, indirect, intentional, negligent, verbal, written, electronic, or inferred through contextual information.

[redacted].

Violations involving TS/SCI information are considered among [redacted]

The TS/SCI clearance therefore represents the highest expression of organizational trust within GCIS. Personnel entrusted with this authorization serve at the forefront of the organization's most sensitive intelligence and [redacted] of discretion, loyalty, professionalism, operational discipline, and security awareness. Their actions directly influence the safety of personnel, the protection of intelligence sources, the success of [redacted], the preservation of strategic partnerships, and the long-term effectiveness of GCIS's most sensitive mission capabilities.

Universal Security Requirements Applicable to All Clearance Holders

Regardless of clearance level, position, directorate assignment, contractual status, or operational role, all personnel granted access to GCIS facilities, systems, information, operations, personnel, or resources are subject to a common set of security obligations designed to protect the integrity of the organization and the safety of those it serves. These requirements form the foundation of the GCIS security program and apply equally to personnel holding General, Secret, Top Secret, and TS/SCI clearances. While higher clearance levels may carry additional responsibilities and restrictions, no clearance holder is exempt from the core principles of confidentiality, operational security, information protection, and professional accountability.

One of the most fundamental principles governing access to information within GCIS is the concept of Need-to-Know. Access to protected information is granted solely on the basis of operational necessity and the performance of authorized duties. Possession of a security clearance does not, by itself, create an entitlement to access information. Personnel must possess both the appropriate clearance level and a legitimate operational, investigative, administrative, supervisory, or support-related requirement before access may be granted. Access may be restricted, modified, suspended, or revoked at any time based upon mission requirements, compartmentation controls, security concerns, or organizational priorities. Personnel are prohibited from seeking, requesting, accessing, reviewing, or retaining information that falls outside the scope of their authorized duties, regardless of curiosity, personal interest, organizational seniority, or technical ability to access such information.

All clearance holders are required to actively protect Operational Security (OPSEC) information and exercise sound judgment in all matters involving sensitive organizational activities. Personnel shall not disclose, discuss, publish, transmit, confirm, deny, acknowledge, or otherwise communicate protected information to unauthorized individuals or entities. This obligation extends to information concerning operational plans, [redacted]. Personnel must recognize that seemingly insignificant pieces of information may become highly sensitive when combined with other information and therefore must remain vigilant against both direct and indirect disclosures. Operational security responsibilities apply equally in professional settings, public environments, digital communications, social interactions, and personal activities.

The protection of digital assets and information systems is likewise a responsibility shared by all clearance holders. Personnel are required to utilize only approved systems, networks, applications, devices, and communications platforms when accessing, processing, storing, or transmitting protected information. Multifactor authentication shall be maintained on all designated systems, and approved encryption technologies shall be utilized whenever sensitive information is stored or transmitted. Personnel must comply with all applicable cybersecurity policies, access-control requirements, device security standards, and information handling procedures. Any actual, suspected, or attempted cybersecurity incident, unauthorized access, credential compromise, malware infection, suspicious activity, or information security concern shall be reported immediately through designated reporting channels. Personnel are expected to maintain awareness of evolving cyber threats and comply with updated security requirements issued by authorized organizational authorities.

The [redacted] represents another essential responsibility of all personnel. Identification cards, access badges, facility keys, security tokens, passwords, passphrases, multifactor authentication devices, facility access codes, and other access credentials are issued on an individual basis and remain the property of GCIS. Personnel shall not share, lend, transfer, disclose, duplicate, or otherwise provide access to any credential or authentication mechanism. No individual may access systems, facilities, applications, or restricted areas using another person's credentials, nor may personnel permit others to operate under their assigned

access privileges. All lost, stolen, compromised, or suspected compromised credentials must be reported immediately so that appropriate security measures may be implemented. The protection of credentials is critical to maintaining accountability, preserving access controls, and preventing unauthorized access to protected resources.

All personnel are further required to maintain the confidentiality of protected information entrusted to them during the course of their service. This obligation extends beyond the active period of employment, assignment, volunteer service, contractual engagement, operational participation, or organizational affiliation. Confidentiality requirements remain in effect following resignation, retirement, reassignment, suspension, contract termination, separation from service, or any other change in organizational status. Personnel shall not disclose, discuss, publish, transmit, or otherwise reveal protected information obtained during their affiliation with GCIS unless specifically authorized to do so by the appropriate authority. The termination of access privileges does not terminate confidentiality obligations.

[redacted].

Personnel are expected to exercise professionalism, discretion, integrity, and sound judgment at all times when handling protected information. The trust placed in clearance holders constitutes a continuing responsibility that extends beyond specific assignments, operational activities, or periods of active service. Every individual granted access to protected information serves as a steward of organizational security and bears personal responsibility for ensuring that information, systems, personnel, and operational activities remain protected from unauthorized access, disclosure, compromise, misuse, loss, or exploitation.

Failure to comply with these universal security requirements may result in administrative action, suspension of access privileges, clearance revocation, reassignment, [redacted], civil liability, internal investigations, [redacted], criminal referral, or any other lawful corrective action deemed necessary to protect the interests of GCIS, its personnel, its partners, and the individuals whose safety depends upon the safeguarding of protected information.

VIOLATION REPROCAUTION TABLE

Severity	Examples	Likely Outcome
Minor	Accidental policy violation, first-time procedural error	Counseling, retraining
Moderate	Unauthorized access attempt, improper storage	Suspension, investigation
Serious	Unauthorized disclosure, credential sharing	Clearance revocation
Critical	Deliberate disclosure of compartmented information, source exposure, operational compromise	Permanent revocation, termination, civil action, criminal referral

Clearance Adjudication Principles

The effectiveness of the Ground Coordination Intelligence Service depends upon its ability to ensure that protected information is entrusted only to individuals who have demonstrated the character, judgment, reliability, and professionalism necessary to safeguard organizational interests. Accordingly, all security clearance determinations shall be based upon a comprehensive evaluation of an individual's suitability for access to protected information, facilities, systems, operations, personnel, and resources. The adjudication process is designed not only to assess current eligibility but also to evaluate an individual's long-term ability to uphold the responsibilities associated with access to sensitive information.

Security clearances are granted only after careful consideration of all available information relevant to an individual's trustworthiness, reliability, and operational suitability. Adjudicators shall consider the totality of circumstances when evaluating an applicant or clearance holder, recognizing that security decisions require a balanced assessment of both favorable and unfavorable information. No single factor shall automatically determine eligibility unless specifically prohibited by law, policy, or organizational directive. Rather, adjudicators shall evaluate whether the individual can be reasonably trusted to protect protected information and act in a manner consistent with the security interests of GCIS.

Among the most important considerations is an individual's demonstrated loyalty to the mission, objectives, values, and lawful obligations of the organization. Personnel entrusted with protected information must consistently demonstrate commitment to the organization's mission and a willingness to place organizational security above personal convenience, personal interests, or outside influences. Loyalty includes adherence to established policies, respect for confidentiality requirements, support for operational security measures, and a commitment to protecting personnel, victims, witnesses, sources, and operational activities from compromise.

Trustworthiness is the cornerstone of every clearance determination. Personnel granted access to sensitive information are often placed in situations where they must independently exercise judgment while handling information that cannot be publicly disclosed or independently verified. Adjudicators shall evaluate whether an individual has demonstrated honesty, transparency, accountability, and ethical conduct throughout their personal and professional history. Acts involving dishonesty, deception, fraud, deliberate policy violations, or abuse of trust may call into question an individual's suitability for access to protected information.

Reliability is equally essential to the clearance process. Individuals entrusted with organizational resources and sensitive information must demonstrate consistent dependability, responsibility, and adherence to professional obligations. Reliability may be assessed through employment history, professional performance, attendance records, disciplinary history, compliance with reporting requirements, and an individual's ability to fulfill assigned responsibilities under routine and stressful conditions alike.

Integrity represents a fundamental requirement for all clearance holders. Personnel are expected to maintain the highest standards of personal and professional conduct regardless of whether their actions are subject to direct supervision. Individuals who demonstrate integrity act honestly, comply with applicable policies and directives, accept responsibility for their actions, and consistently place ethical considerations above personal gain. Integrity serves as a critical indicator of an individual's ability to responsibly manage sensitive information and maintain organizational trust.

The exercise of sound judgment is another critical adjudicative factor. Clearance holders routinely encounter circumstances requiring discretion, risk assessment, and decision-making in environments where mistakes may have significant consequences. Adjudicators shall evaluate an individual's history of decision-making, problem-solving, and professional conduct to determine whether they possess the maturity and judgment necessary to responsibly handle protected information and operational responsibilities.

Operational discretion is particularly important for personnel whose duties involve sensitive investigations, intelligence activities, operational planning, or compartmented information. Personnel must demonstrate the ability to maintain confidentiality, exercise restraint in communications, recognize security risks, and avoid disclosures that could compromise personnel, investigations, sources, victims, operations, or organizational capabilities. A demonstrated history of careless disclosures, inappropriate public communications, or disregard for confidentiality obligations may weigh heavily against clearance eligibility.

Security awareness and cybersecurity competence are increasingly important components of the adjudication process. Personnel entrusted with access to organizational systems and information must understand modern security threats and demonstrate the ability to comply with applicable information security requirements. Adjudicators may consider an individual's cybersecurity practices, understanding of operational security principles, history of compliance with security procedures, and willingness to report security incidents or vulnerabilities. Personnel who demonstrate negligence in safeguarding digital resources or who repeatedly violate security protocols may be deemed unsuitable for continued access.

An individual's demonstrated ability to safeguard protected information is a central consideration in all clearance decisions. Personnel must consistently show that they understand the responsibilities associated with access to sensitive information and possess the discipline necessary to protect it from unauthorized disclosure, loss, misuse, compromise, or exploitation. This assessment may include review of prior security incidents, information handling practices, reporting compliance, operational conduct, and overall security performance.

Adjudicators shall also consider an individual's compliance history when evaluating eligibility for initial or continued access. Compliance history includes adherence to organizational policies, reporting requirements, security directives, operational procedures, confidentiality obligations, and applicable legal requirements. Repeated violations, failure to

report relevant information, unauthorized disclosures, or disregard for established security controls may indicate an elevated security risk and may adversely affect adjudicative outcomes.

Finally, every clearance determination shall consider the principle of operational necessity and need-to-know. Access to protected information shall only be granted when a legitimate organizational requirement exists. The existence of eligibility alone does not create a justification for access. Rather, individuals must demonstrate a continuing operational, investigative, administrative, supervisory, technical, or support-related need for the information, systems, facilities, or resources to which access is requested. Access may be reduced, modified, suspended, or revoked when operational necessity no longer exists.

Security clearances are privileges granted in the interest of organizational security and mission effectiveness. No individual possesses an inherent right to a clearance, nor does prior access guarantee continued eligibility. The granting, maintenance, suspension, or revocation of a clearance remains a discretionary security determination based upon organizational trust, operational necessity, risk management considerations, and the individual's continuing ability to protect protected information.

All clearance holders are expected to maintain the standards upon which their access was granted throughout the duration of their affiliation with GCIS. Eligibility for access is a continuing responsibility rather than a one-time determination. Personnel must therefore remain vigilant in safeguarding information, complying with security requirements, reporting relevant concerns, and conducting themselves in a manner consistent with the trust placed in them by the organization. When questions arise concerning an individual's suitability, the protection of personnel, operations, victims, witnesses, sources, and protected information shall remain the paramount consideration in all adjudicative decisions.

Source: Official NDA of GCIS (June 2, 2026).

GROUPS CLEARANCE BASED ON AFFILIATED GROUP ASSIGNMENT

While assignment to certain positions within the Ground Coordination Intelligence Service (GCIS) may, in limited circumstances, result in the automatic issuance of a designated security clearance, such instances are the exception rather than the standard. Automatic clearance assignment is generally reserved for personnel selected for highly specialized assignments, task groups, operational programs, or other [redacted] initiatives where immediate access is deemed necessary for mission effectiveness. Such determinations are made on a case-by-case basis and only when authorized at the discretion of the Director of GCIS.

This policy reflects the GCIS principle that security clearances are primarily granted based on demonstrated operational necessity, access requirements, and organizational need rather than position title alone. As a result, the vast majority of personnel, regardless of rank, leadership status, or occupational specialty, do not receive a predetermined clearance level solely because of the role they occupy.

The only positions within GCIS that are automatically assigned a specified clearance level by virtue of office are the [redacted] Due to the scope of their responsibilities and their requirement to maintain unrestricted access to the Service's most sensitive intelligence, operational, and protective information, individuals serving in [redacted] positions are automatically granted Top Secret/Sensitive Compartmented Information (TS/SCI) access under the [redacted] classification structure.

Apart from these five executive-level offices and any temporary exceptions authorized for designated special assignments or programs, no GCIS member is guaranteed a specific clearance level solely on the basis of their title, department, or organizational placement. Clearance eligibility and access authorizations remain subject to mission requirements, adjudicative standards, and the principle of least privilege, ensuring that individuals are granted access only to the information necessary to perform their assigned duties.

Below are the charts.

AUTOMATIC ISSUANCE OF CLEARANCE LIST		
D[redacted]		
S[redacted] (S[redacted]		
T[redacted]	[REDACTED]	

AUTOMATIC ROLE ISSUANCE OF CLEARANCE		
[REDACTED]		