CAROUSEL CONSULTING, LLC
700 12TH STREET, NW, STE. 700
WASHINGTON, DC 20006

WEBSITE: www.carousel.one
EMAIL: AUDREY@CAROUSEL.ONE
PHONE: (202) 924-8919

M E M O R A N D U M

TO: [REDACTED]
FROM: Audrey Wright Glenn, Head of Legal, Enforcement, Assessment & Development
DATE: October 20, 2026
SUBJECT: *Engagement Governance, Conflicts and Restricted-Information Handling*

CONFIDENTIAL – SUBMITTED FOR LEGAL CONSULTATION AND EVALUATION

I. QUESTIONS PRESENTED

1. *Classification and Acquisition Framework: What statutory, executive, and regulatory authorities govern the establishment, administration, and acquisition flow-down requirements of Special Access Programs (SAPs) and Special Access Required (SAR) environments under the Federal Acquisition Regulation (FAR) and Defense FAR Supplement (DFARS)?*

2. *Third-Party Review and Subcontractor Onboarding: When a commercial contractor serving as a subcontractor must engage an external third party (e.g., outside counsel or alternative legal service provider) to review a prime contract or subcontract containing classified or SAP-governed requirements, what security and procurement protocols must attach prior to disclosure?*

3. *Legal Professional Responsibility and Conflicts of Interest: How do the professional ethics mandates of ABA Model Rules 1.6 and 1.7, Organizational Conflicts of Interest (OCI) rules under FAR Subpart 9.5, and national security non-disclosure obligations intersect when an attorney or firm identifies a non-disclosable conflict, and what is the proper remediation protocol?*

4. *Accession and Legal Consultation Boundaries: What is the lawful procedure for an individual nominated for, or inadvertently exposed to, an SAP to be formally read in, and may that individual consult private legal counsel prior to engaging the government without violating federal criminal statutes?*

5. *The "Orphaned Compartment" and Lawful Dissemination: If an individual understands that a concluded or highly compartmentalized program requires reporting upon a specified event, what authorities establish whether that obligation exists and remains effective, and what authorized procedures permit compliance without an unauthorized disclosure?*

II. SHORT ANSWERS

1. SAP establishment is addressed by Executive Order 13526, § 4.3; 10 U.S.C. § 119 addresses DoD SAP oversight. Section 3093 of Title 50 concerns covert actions, not all intelligence-related SAPs. Applicable security requirements include 32 C.F.R. Part 117 and relevant agency and program directives. In acquisitions, FAR Subpart 4.4, FAR 52.204-2, and applicable DD Form 254 requirements must be assessed against the contract. FAR 52.244-6 identifies mandatory commercial subcontract clauses and permits a minimal number of additional clauses necessary to satisfy contractual obligations; commercial status is not a blanket exemption from additional requirements.

2. Before disclosure to an external reviewer, verify applicable entity and personnel eligibility, need-to-know, program-specific access approval, contractual security documentation, and approved facilities and transmission methods through the responsible security authority. NISS supports facility-clearance verification and DISS supports personnel-security functions; neither substitutes for program authorization or provides a general document-transmission channel. DD Form 254 requirements depend on the classified subcontract and applicable rules. Commercial intake and billing information must also be approved for disclosure; neither a generic description nor a secure location independently establishes authorization.

3. Applicable professional-conduct and security requirements may restrict disclosure of client identities, program names, or conflict details. Suspend affected review and restrict access as appropriate without demanding protected information. Preserve relevant records and logs, and obtain counsel's and the responsible security authority's direction before any return, deletion, sanitization, or destruction. Determine applicable reporting duties and whether screening, consent, withdrawal, or other measures are legally available; screening does not cure every conflict.

4. SAP access requires approval under applicable government and program procedures, including eligibility, need-to-know, and any required program-specific authorization; Top Secret eligibility and a billet are not universal prerequisites for every SAP. Individuals may seek procedural legal advice without disclosing protected information or associations. Attorney-client privilege does not itself authorize disclosure of classified information. Unauthorized disclosure may result in criminal liability, depending on the applicable statute, information, conduct, and mental-state elements.

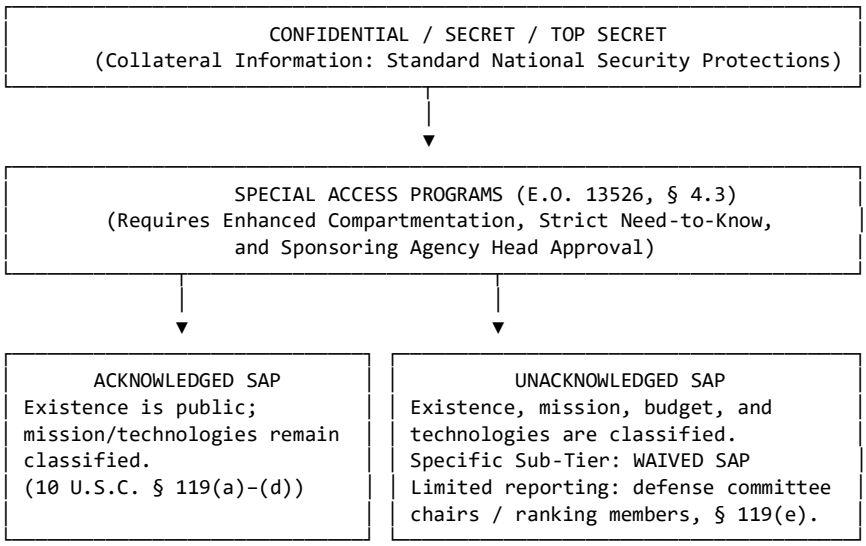
5. Participation in a program does not itself confer declassification or dissemination authority. E.O. 13526, § 3.1 recognizes multiple declassification authorities; declassification and authorized dissemination are distinct. Counsel should first verify any asserted continuing reporting obligation and identify an authorized initial-contact procedure that does not itself disclose protected information or associations. The appropriate receiving authority and channel must be confirmed; neither an administrative pointer nor contact with a SAPCO, DOPSR, or a government attorney creates a disclosure safe harbor.

III. STATUTORY, REGULATORY, AND ACQUISITION FRAMEWORK

A. Constitutional and Executive Classification Hierarchy

The protection of national defense information and the creation of Special Access Programs derive from the President's constitutional authority as Commander-in-Chief (U.S. Const. art. II, § 2) and are formally codified in Executive Order 13526 (Classified National Security Information):

EXECUTIVE CLASSIFICATION TIERS



1. Statutory Oversight of DoD SAPs (10 U.S.C. § 119): Section 119 establishes reporting requirements to the congressional defense committees. Under § 119(e), the Secretary may waive a requirement under subsections (a), (b), or (c) upon the specified determination; the required information is then provided to the chair and ranking minority member of each defense committee. This is not the intelligence "Gang of Eight" reporting arrangement, and waiver is not synonymous with unacknowledged status.

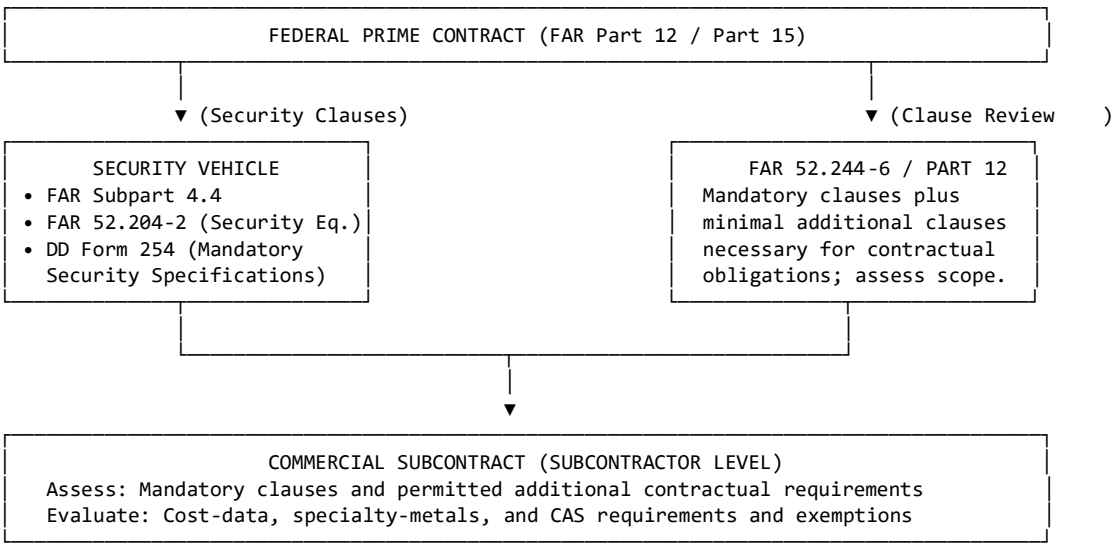
2. Intelligence Community Authorities: Counsel should identify the authorities applicable to the particular program. ICD 115 addresses the Intelligence Community Capability Requirements Process, not a general SAP-governance framework. 50 U.S.C. § 3093 addresses presidential approval and reporting of covert actions and does not govern all intelligence-related SAPs.

3. Operational Security Manuals: Day-to-day administrative and physical security execution is governed by:

- 32 C.F.R. Part 117: The National Industrial Security Program Operating Manual (NISPOM Rule).
- DoD Directive 5205.07 & DoD Manual 5205.07 (Vols. 1–4): DoD Special Access Program Security Manual (covering personnel, physical, information, and IT security in SAP environments).
- ICD 705 / Technical Specifications: Standards for the construction and accreditation of SCIFs and SAPFs.

B. The Federal Acquisition Framework: FAR & DFARS Flow-Downs

In procurement, classified requirements enter transactions through specialized clauses that interface with the supplier's commercial baseline:



1. **FAR Subpart 4.4 & FAR 52.204-2 (Security Requirements):** Requires prime contractors and subcontractors to maintain a system of security controls compliant with the NISPOM (32 C.F.R. Part 117).

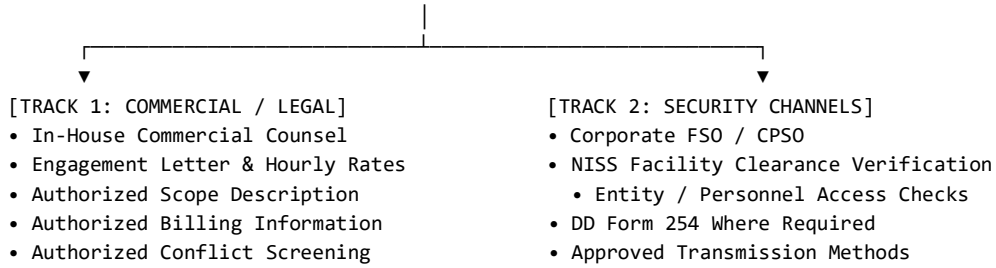
2. **DD Form 254 (DoD Contract Security Classification Specification):** Where required, this form specifies contractual classification and security requirements. It does not independently confer access authorization; applicable entity and personnel eligibility, need-to-know, program approvals, safeguarding capability, and transmission requirements must also be satisfied.

3. **Commercial Subcontract Flow-Down Review (FAR 52.244-6 & DFARS 252.244-7000):** Review each proposed flow-down against the applicable contract, clause version, commercial-product or commercial-service status, and relevant exemptions. FAR 52.244-6 identifies mandatory clauses and permits a minimal number of additional clauses necessary to satisfy contractual obligations. The following clauses require applicability review rather than categorical acceptance or rejection:
   - FAR 52.204-25: Prohibition on Contracting for Certain Telecommunications and Video Surveillance Equipment (Section 889 NDAA).
   - FAR 52.204-27: Prohibition on a ByteDance Covered Application (TikTok).
   - FAR 52.204-30: Federal Acquisition Security Council (FASC) Exclusion Orders.
   - DFARS 252.204-7012: Safeguarding Covered Defense Information and Cyber Incident Reporting (NIST SP 800-171 compliance, applicable where Covered Defense Information is processed on contractor systems).

IV. SUBCONTRACTOR GOVERNANCE & THIRD-PARTY ONBOARDING

Commercial administration and security authorization should be coordinated when retaining an external reviewer. The two-track model below is an organizational approach, not a universally mandated protocol; the responsible security authority must confirm applicable requirements before disclosure.

EXTERNAL CONTRACT REVIEW ONBOARDING



A. The "Two-Track" Governance Protocol

1. Track 1 (Commercial/Legal): Establishes engagement terms, fees, nondisclosure obligations, and invoice administration. Any scope description and billing information must be authorized for the intended recipients. A generic or “sterile shell” description does not itself establish that protected information or associations have been removed.

2. Track 2 (Security): Appropriately authorized security personnel coordinate with the responsible government security authority to verify applicable requirements, including:

- Verifying the outside firm's Commercial and Government Entity (CAGE) Code;
- Validating required entity eligibility and safeguarding capability through the cognizant authority; NISS supports DCSA facility-clearance verification;
- Confirming personnel eligibility, need-to-know, and required program-specific access; DISS supports personnel-security functions; and
- Completing applicable contractual security documentation, including a sub-tier DD Form 254 where required, and confirming approved facilities and transmission methods.

B. Special Access Program (SAP) In-SCIF Containment

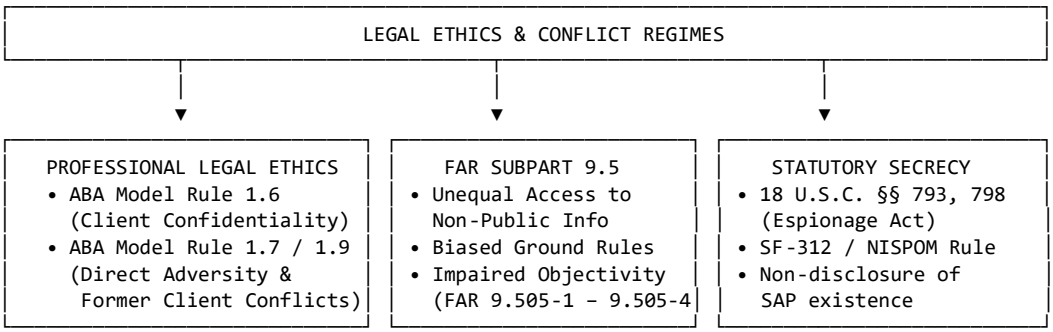
Access to substantive program terms depends on the recipient’s authorization, not merely their commercial or legal role. Unacknowledged-program information must be handled under applicable program instructions.

- Program Access Authorization: A clearance alone does not authorize SAP access. Verify the applicable eligibility level, need-to-know, and program-specific approval, including any required billet or access request, through the responsible security authority.
- Approved Facilities: Conduct classified review only in facilities and systems approved for the particular information and activity. Accreditation as a SCIF or SAPF does not by itself establish authorization for every program.
- Review of Legal Outputs: Determine classification and authorized dissemination under applicable guidance. Only outputs confirmed as suitable for the specific recipients may be released; removing code words or using generalized commercial instructions does not itself establish that the information is unclassified or releasable.

V. LEGAL ETHICS, CONFLICTS OF INTEREST, AND SILENT CONFLICT MITIGATION

A. The Intersection of ABA Model Rules and Federal Secrecy Laws

When a third-party reviewer evaluates a prime contract on behalf of a subcontractor, the engagement interfaces with three overlapping regulatory bodies:



1. The Doctrine of the "Silent Conflict":

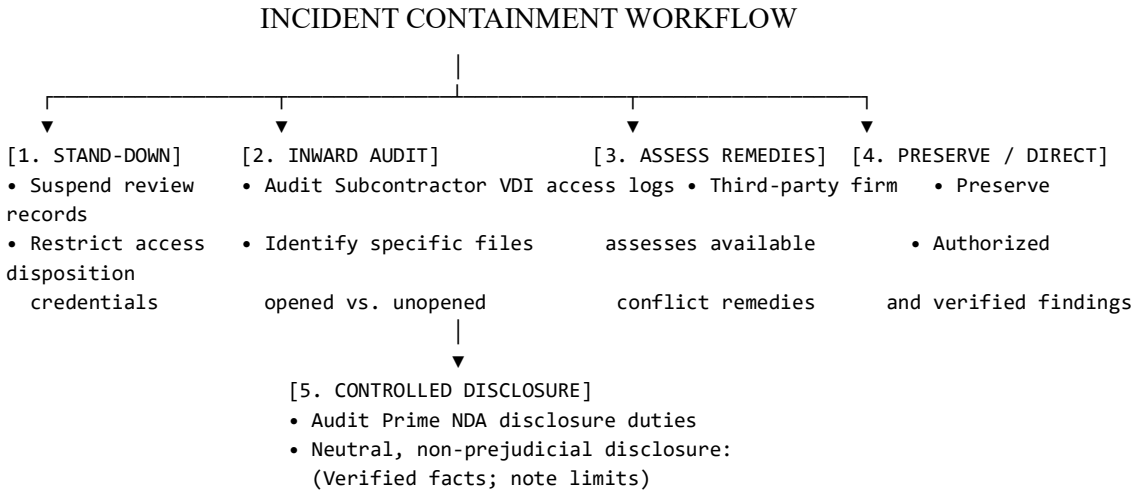
Under ABA Model Rule 1.6, an attorney owes a duty of strict confidentiality to all clients. Where an outside firm is conflicted because it represents the Prime Contractor or a competing bidder on the same procurement, the mere disclosure of the other client's identity or bidding intent may constitute a professional ethics violation. Unauthorized disclosure of protected program information may result in criminal liability, depending on the applicable statute and facts.

2. Organizational Conflicts of Interest (OCI) (FAR 9.505-4):

Access to proprietary bid or proposal data or non-public source-selection information may raise an unequal-access OCI, depending on the facts and applicable procurement rules. FAR 9.504 requires assessment and appropriate avoidance, neutralization, or mitigation; exclusion may result where a significant conflict cannot be addressed, subject to applicable procedures and waiver authority. Disqualification of both prime and subcontractor is not automatic.

B. Incident Response Considerations: Assignment Before Conflict Screening

If an external reviewer identifies a conflict after assignment, suspend affected review and restrict access as appropriate. The following workflow identifies issues for counsel and the responsible security authority; it is not a universally mandated sequence or timetable. Preserve records and logs, assess reporting duties, and obtain direction before any return, deletion, sanitization, or destruction.



Phase 1: Suspend Review and Restrict Access as Appropriate

- Issue an immediate, written Stop-Work Directive instructing the reviewer to halt all review, copying, distribution, or discussion of the contract package.
- Coordinate appropriate access restrictions with IT Security while preserving accounts, relevant records, and access logs.

Phase 2: Preserve and Assess Access Evidence

- Recognize that the reviewer's declination is conclusive and non-negotiable; in-house counsel must not attempt to compel disclosure of the conflicted client's identity or classified program details.
- Pivot the investigation inward: Preserve and assess access logs and other evidence to evaluate possible exposure:
  - Did the reviewer open substantive pricing exhibits, technical SOWs, or bills of materials?
  - Did the reviewer disconnect immediately upon reviewing the title page or party names?
- Preserve an evidentiary audit trail documenting actual access and any unresolved limitations; do not presume absence of exposure.

Phase 3: Assess Available Conflict Remedies and Quarantine

- Have responsible counsel determine whether screening is permitted and sufficient under applicable rules, or whether consent, withdrawal, or another measure is required. Where a screen is appropriate, measures may include:
  - Barring the exposed reviewer personnel from communicating with or advising the firm personnel working on the conflicting matter; and
  - Restricting internal firm document systems to ensure the relevant files cannot be accessed by other firm personnel.

Phase 4: Obtain Direction on Disposition and Document Verified Facts

- Obtain counsel’s and the responsible security authority’s direction before return, deletion, sanitization, or destruction. Any written confirmation must be supported by verified facts and address, as applicable:
  1. The review suspension, withdrawal, or other engagement measures actually taken;
  2. Preservation and authorized disposition of files, cached emails, working notes, and relevant logs, subject to retention and evidence-preservation duties;

3. Verified findings concerning access, use, or disclosure, including any unresolved limitations; and
4. Any screening, consent, participation restrictions, or withdrawal determined necessary under applicable rules.

Phase 5: Controlled Upstream Notification

- Audit the Prime Contractor Non-Disclosure / Teaming Agreement. If a reporting duty is triggered, the disclosure must be factual, controlled, and non-prejudicial:

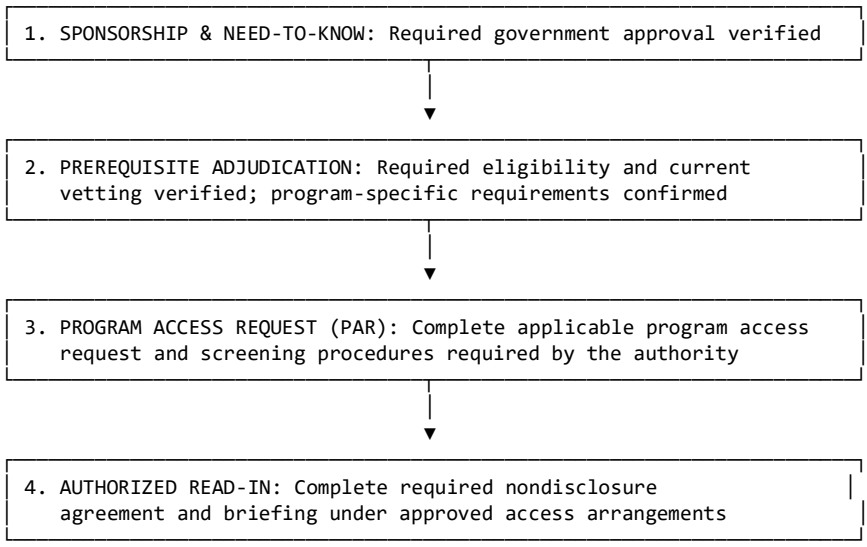
  Any required notification should state only verified facts concerning the assignment, identified conflict, access restrictions, preserved evidence, and authorized remedial measures. Distinguish confirmed findings from matters still under review. Do not certify deletion, absence of disclosure, or "zero taint" unless established; exclude protected client or program information unless disclosure is authorized.

VI. SAP ACCESSION, READ-IN PROTOCOLS, AND LEGAL COUNSEL CONSULTATION

A. The Accession Architecture

Access to Special Access Programs is governed by strict procedural prerequisites designed to eliminate personal discretion:

THE SAP READ-IN PIPELINE



- Inadvertent Exposure (Spillage): Possible unauthorized receipt does not confer a right to program access. Avoid further unauthorized disclosure, preserve relevant evidence, and promptly seek instructions through an established authorized security contact under applicable reporting procedures. Do not independently delete or sanitize material. Section 117.14 concerns marking; reporting and response obligations must be assessed under applicable NISPOM and program requirements.

B. Seeking Legal Counsel Prior to Engaging the Government

Individuals navigating clearance processing or inadvertent exposure frequently seek private counsel. However, the legal scope of that consultation is severely restricted by federal criminal law:

Procedural Legal Consultation Topics *(Subject to applicable disclosure restrictions)*	**Disclosures Requiring Authorization** *(Potential criminal liability)*
How to answer personal background, financial delinquency, or drug questions on an SF-86 or PSQ.	Disclosing classified program code words, operational targets, or technical network specifications without authorization.
Advising on personal liability, self-incrimination, and Fifth Amendment protections.	Transmitting or displaying classified contract schedules, SOWs, or DD Form 254s to counsel who is not authorized to receive the particular information.
Explaining procedural rights under the NISPOM or Defense Office of Hearings and Appeals (DOHA).	Disclosing protected information identifying an unacknowledged agency sponsor or program compartment without authorization.
Whistleblower procedural rights under 50 U.S.C. § 3234 and DoD Inspector General reporting channels.	Attorney-client privilege does not itself authorize disclosure of classified information.

- Potential Criminal Liability (18 U.S.C. §§ 793, 798): Liability depends on the applicable statute's information, conduct, and mental-state elements. Section 798 addresses specified classified communications-intelligence and related information, not every classified disclosure. Counsel must be authorized to receive the particular information; clearance alone is insufficient. Attorney-client privilege does not itself authorize disclosure of classified information.

- Authorized Counsel Access: Where classified facts are necessary for legal advice or representation, identify the applicable process for counsel's eligibility, need-to-know, program-specific authorization, and approved access arrangements. Administrative clearance proceedings and federal criminal proceedings may involve different procedures:

- In federal criminal proceedings, the Classified Information Procedures Act (CIPA, 18 U.S.C. App. III) governs specified procedures for classified information, subject to court orders and applicable security arrangements. It is not a general access mechanism for private consultation or administrative clearance proceedings.

VII. THE "ORPHANED COMPARTMENT" AND LAWFUL DISSEMINATION OF ACTIONABLE INTELLIGENCE

A. The Structural Problem

An individual may understand that obligations arising from a concluded or highly compartmentalized program require delivery of information upon a specified event. Counsel must first verify the asserted obligation, its source, continuing effect, and authorized recipient; this memorandum does not establish that such a duty exists. The issues for evaluation include: (1) a perceived affirmative duty to deliver the intelligence they were engaged to gather; and (2) applicable restrictions on disclosure, including protected program identities, associations, and substantive information.

B. The Fallacy of Personal Release Authority

Program participation does not itself confer declassification or release authority. E.O. 13526, § 1.3 addresses original classification; § 3.1 recognizes multiple declassification authorities, including specified successors, supervisors, and delegated officials. Declassification and authorization to disseminate are distinct and must be evaluated separately.

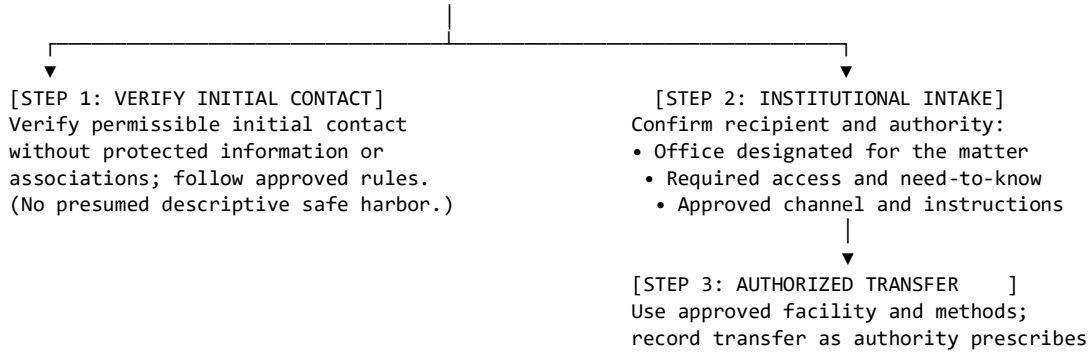
- Where SF-312 applies, its continuing nondisclosure obligations and authorization provisions must be assessed according to its terms; counsel should verify the agreement and its applicability rather than assume every participant signed it.

- Unilateral release through automated mechanisms, commercial cloud storage, or unauthorized recipients may violate applicable obligations and may result in criminal liability depending on the statute and facts. Benign motives do not themselves authorize disclosure.

C. Verification of Authorized Contact and Intake Procedures

No general “blind pointer” safe harbor is established by the cited authorities. Counsel should determine an authorized initial-contact procedure that does not itself disclose protected information or associations. An administrative description, secure facility, or government recipient’s title does not independently establish disclosure authorization. The diagram below identifies verification steps, not permission to transmit information.

AUTHORIZED CONTACT / INTAKE VERIFICATION



1. Verification of the Appropriate Receiving Authority

- **The Cognizant Department SAP Central Office (SAPCO):** For a DoD matter, confirm through established authorized security channels whether the DoD SAPCO or another designated office is the appropriate contact; do not presume its authority to receive particular substantive information. A service SAPCO may be relevant where the responsible authority confirms its jurisdiction and provides approved initial-contact instructions. For a DOE-related matter, confirm the cognizant office and its jurisdiction under applicable authorities before any substantive disclosure.

- **Intelligence Community Matters:** Verify the responsible agency or ODNI office, its jurisdiction, and the approved contact procedure. ICD 115 concerns capability requirements, not general SAP intake authorization.

- **Agency Legal Counsel:** An agency counsel's title or clearance does not alone establish authority to receive particular information. Confirm the appropriate recipient, need-to-know, program authorization, and approved communication arrangements.

2. Applicable Prepublication and Security Review

Where a proposed public or industry release is subject to prepublication or security review:

- Determine the applicable review obligation and receiving office. DOPSR under DoDI 5230.09 or the relevant agency review process may apply; obtain approved submission instructions before transmitting potentially classified material. DOPSR is not a universal intelligence-intake channel.

- Any written release determination applies only to the material, purpose, and conditions covered by that determination; it does not establish blanket immunity or resolve unrelated legal obligations.

3. Documentation of Authorized Transfers

Document any authorized transfer using the receiving authority's prescribed receipt or acknowledgment. DD Form 1907 is a Signature and Tally Record, not a universal receipt requirement for legal consultation or intelligence intake.

- Record the transfer details required by the authorized receiving procedure, using only identifiers appropriate for the record's classification and handling restrictions.

- The record may evidence the transfer but does not independently establish its legality or satisfaction of all reporting obligations.

VIII. SUMMARY

- ***Review Commercial Flow-Downs***: Evaluate each proposed clause under the applicable contract, clause version, commercial status, and relevant exemptions. FAR 52.244-6 identifies mandatory clauses and permits a minimal number of additional clauses necessary to satisfy contractual obligations. Do not categorically reject cost-data, audit, or other requirements solely on commercial status.

- ***Verify Security Authorization Before Disclosure***: Coordinate with appropriately authorized security personnel and the responsible government authority to confirm entity and personnel eligibility, need-to-know, program approvals, contractual security documentation, and approved facilities and transmission methods. NISS and DISS serve distinct security-administration functions; neither substitutes for program approval or constitutes a general transmission channel. Section 117.13 concerns classification, not the complete onboarding process.

- ***Conduct Security-Authorized Conflict Checks:*** Before disclosing information to a prospective legal or consulting reviewer, obtain direction from the cognizant government program security authority, coordinated through appropriately authorized security personnel, regarding permissible disclosures, recipients, and communication channels. Do not assume that a Prime Contractor's name, an unclassified agency code, or their association with a particular matter may be disclosed; identifying information or its contextual association may reveal protected program information, including the existence of an unacknowledged SAP. Limit preliminary screening to information authorized for disclosure to the particular recipient. Before providing classified information, verify the recipient's eligibility, need-to-know, and any required program-specific access authorization, and use approved facilities and transmission methods. A generalized or blind conflict certification does not substitute for an adequate conflicts assessment under applicable professional rules. If adequate screening cannot be completed without an unauthorized disclosure, pause the engagement pending an authorized resolution.

- ***Respond to Identified Conflicts Without Demanding Protected Details***: Suspend affected review and restrict access as appropriate. Preserve relevant records and logs; obtain counsel's and the responsible security authority's direction before return, deletion, sanitization, or destruction. Assess reporting duties and whether screening, consent, withdrawal, or other remedies are available. Any notification or certification must distinguish verified facts from unresolved findings.

- ***Maintain Security Boundaries During Legal Consultation***: Attorney-client privilege does not itself authorize disclosure of classified information. Do not assume an administrative pointer, personal-status description, or program-related request is unclassified or authorized for transmission. Verify any asserted continuing reporting duty and obtain approved initial-contact instructions through an established authorized security contact. Confirm the receiving authority, need-to-know, program approval, facility, and channel before substantive disclosure. Use prepublication review only where applicable and document authorized transfers as prescribed; neither release review nor a receipt creates blanket immunity.