FAST-TRACKING ACQUISITION SECURITY TRANSFORMATION (FAST) STUDY REPORT

Accelerating secure innovative acquisitions to empower warfighter and expand the Defense Industrial Base

December 2025

For questions, feedback, or more information, please contact
Dr. Deanna D. Caputo (dcaputo@mitre.org) and Dr. James Doodson (doodsonj@mitre.org)

The view, opinions, and/or findings contained in this report are those of The MITRE Corporation and should not be construed as an official Government position, policy, or decision, unless designated by other documentation. This technical data deliverable was developed using contract funds under Basic Contract No. W56KGU-18-D-0004.

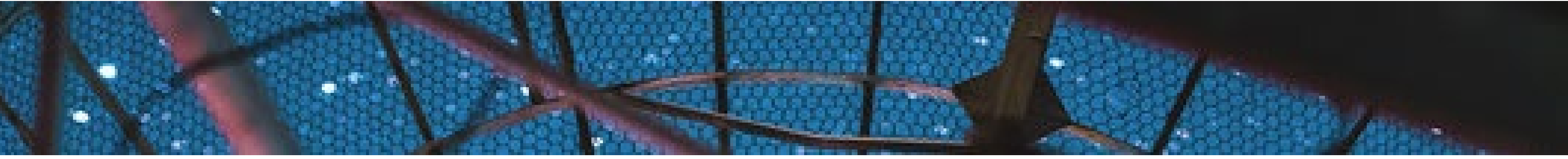
MITRE | National Security Engineering Center

TABLE OF CONTENTS

LIST OF TABLES AND FIGURES

Tables

Figures



EXECUTIVE SUMMARY

The Department of War (DOW) is executing once-in-a-generation acquisition reforms that demand wartime speed and a larger, more diverse defense industrial base (DIB). In parallel, the DOW must transform security requirements, policies, and practices built for a paper-based and facility-centric environment. In support of these reforms, the MITRE Fast-tracking Acquisition Security Transformation (FAST) Study analyzed how current security requirements, policies, and practices affect the DIB's speed, cost, and schedule to effectively deliver on DOW acquisition.

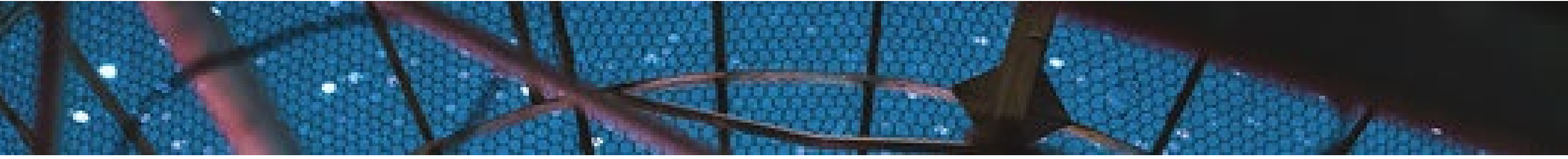
The premise of the FAST Study is that the National Industrial Security Program (NISP), established in 1993, was designed for a vastly different era of DOW acquisition practices, systems, DIB composition, and threat environment, and that in the intervening 32 years little has changed in its overall framework. Today, classified and sensitive information is created, processed, and transmitted in dynamic, distributed digital systems, while many industrial security processes still operate as if information remains stationary, paper-based, and confined to fixed facilities. DOW is preparing to implement major changes such as NDAA Section 847 and rely more heavily on small businesses and nontraditional defense contractors (NDCs) that cannot absorb long delays or opaque processes. At the same time, the threat environment has intensified, with adversaries actively targeting the DIB to steal technologies, exploit foreign ownership, control, or influence (FOCI), and disrupt supply chains. Now is the time to optimize DOW's *acquisition security* approach so that NISP requirements, Controlled Unclassified Information (CUI), and other frameworks are justified, measurable, fit-for-purpose, and aligned with the Department's wartime footing and rapid acquisition reforms.

Methodology

The FAST Study was designed as a targeted, systematic, deep-dive analysis of DOW security requirements, practices, and systems that impact the DIB's ability to quickly, affordably, and successfully enable the warfighter mission. Between July and November 2025, MITRE's behavioral sciences and security researchers collected quantitative and qualitative data from 6,734 security industry leaders, practitioners, and innovators across 105 organizations.

Industry Type	Number
Defense Contractors	65
• Small Businesses	28
• Medium-sized Businesses	7
• Large-sized Business	18
• Academic Institutions	12
NDCs	5
Security-as-a-Service Providers	21 (representing 3269 industry companies)
Council/Consortiums	14 (representing 3360 industry companies)

Data was gathered through semi-structured interviews, online questionnaires, and focus groups, then analyzed using thematic analysis and descriptive statistics to identify persistent challenges, quantify burden in time, cost, and workforce hours, and distinguish anecdotes from systemic issues. All identified acquisition security challenges and recommended government actions were cross-referenced with publicly available laws, regulations, directives, manuals, and oversight reports to ensure alignment with current authorities and to prioritize options that reduce burden, expand access, and maintain or improve security outcomes.



Findings and Recommendations

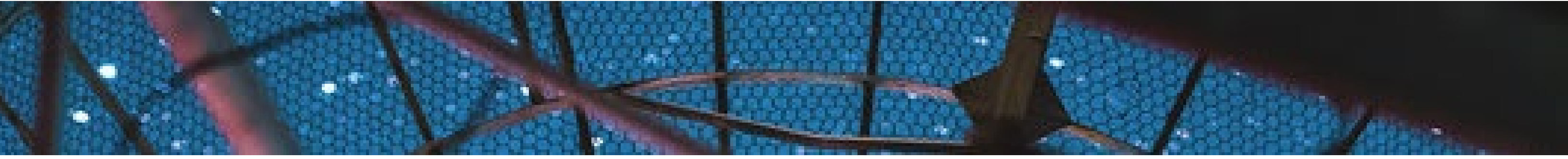
Based on experiences from 6,734 companies, the MITRE FAST Study identified 74 acquisition security challenges across five focus areas: (1) Entity Eligibility and Access, (2) FOCI, (3) Safeguarding of Classified and Sensitive Information, (4) Cybersecurity, and (5) Integration of Security into Acquisition Processes and Contracts. The acquisition security challenges in those focus areas were rarely due to gaps in law or basic policy; law and policy appear broad enough to enable the flexibility of mission requirements and rapid on-the-ground decision-making. Instead, challenges arose from interpretation, sequencing, and implementation of existing requirements, policies, and practices. Security processes designed for a different era now slow delivery, discourage new entrants, and produce inconsistent outcomes. As DOW rapidly moves toward a wartime footing and dramatically accelerates the fielding of new technology and advanced capabilities to maintain US military superiority, these challenges will intensify. Each of the 75 challenges is accompanied by one of 155 recommended government actions.

1. **Entity Eligibility and Access:** Entity Eligibility is the critical entry point for classified DIB contracts, yet interviewees described DCSA's self-ascribed "America's Gatekeeper" role as successfully preventing DOW from growing the DIB with new innovative technology companies. Interviewees also consistently described DCSA having a "checklist mentality," confusing new entrants with Facility Clearance terminology, and requiring manual, non-automated processes that create barriers to entry and delay project starts, especially for NDCs, small, and medium-sized businesses. NISS was clearly described as unsuitable for 21st century business when, for example, change-condition "lock outs" create long holds and duplicative submissions for additional sites, and CAGE codes drive backlogs. Government Contracting Agencies are often not willing or do not understand how to sponsor companies for Entity Eligibility, and rarely provide DD-254s during solicitation or proposal submission phases.

   For example, the FAST Study recommends:

   - DCSA shift from a gatekeeping culture to a warfighter service provider culture.
   - OUSW(I&S) retire the term Facility Clearance and replace it with Entity Clearance-Eligibility and Entity Clearance-Access.
   - More DD-254s be prepared and released no later than solicitation.
   - DCSA employ or partner with plain-English automation tools (e.g., TurboFCL and NISS Increment II) to triage packages, support multiple concurrent change conditions, and provide graphical status tracking.
   - OUSW(I&S) allow trusted DIB companies with superior security ratings to self-certify additional sites for interim eligibility.
   - OUSW(I&S) align personnel and entity eligibility timeframes to five years to rapidly, but safely, expand the pool of eligible companies and personnel ready to rapidly support classified work.

2. **FOCI:** Across industry interviewees, FOCI is recognized as a real risk that must be managed, however, the current approach is viewed as outdated, overly burdensome, and insufficiently risk-based, particularly for globally funded and FOCI-mitigated companies that must overcome negative perceptions and additional costs and delays. Completing and maintaining SF-328s requires months of effort; the review and mitigation process commonly takes 40 weeks or more; mitigation agreements and supplemental policies take many months to years to receive final approval; and Outside Directors and Government Security Committees are insufficiently empowered to make routine decisions that could be handled without DCSA approval.



For example, the FAST Study recommends:

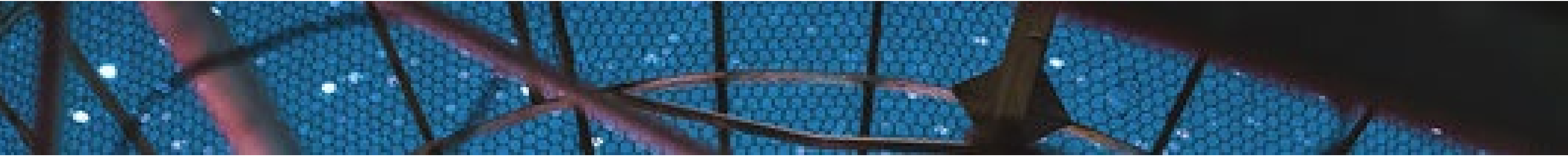
- DCSA implement automated SF-328 error checking and triage, update Industrial Security Letters to clarify “material change” and modern ownership models, and require that SF-328s be submitted only to DCSA.
- Training acquisition officials to consider mitigation status and security ratings rather than treating all FOCI as an unmitigated risk.
- Reusing validated CMMC artifacts for overlapping Electronic Communications Plan (ECP) controls and streamlining Affiliated Operations Plan (AOPs) through risk-based playbooks.
- Immediately issuing clear NDAA Section 847 implementation guidance (especially on the $5M threshold).
- Funding a comprehensive FOCI study to evaluate return-on-investment, mitigation effectiveness, and reciprocity across Cognizant Security Agencies.

3. **Safeguarding of Classified and Sensitive Information:** The FAST Study finds that programs routinely begin and move through key acquisition milestones without early, authoritative identification of Critical Program Information (CPI), Controlled Technical Information (CTI), CUI, and classification boundaries, and that Program Protection Plans (PPPs), Security Classification Guides (SCGs), CUI annexes, and DD-254s frequently arrive after architectures and teaming arrangements are set. CUI policy was also found to be implemented inconsistently across DOW and government personnel sometimes mishandle CUI when engaging with industry. Lastly, SCIF accreditation timelines, reciprocity, and co-use are uneven and unpredictable, which forces redundant facilities, constrains access for subcontractors and new entrants, and delays the start of classified work.

   For example, the FAST Study recommends:

   - DOW establish a mandatory Program Protection Baseline as a gating artifact prior to acquisition strategy approval and solicitation release, and issue a single, authoritative DOW CUI Marking and Dissemination Profile.
   - DOW enforce SCIF reciprocity and co-use supported by a Department-wide Accredited Classified Space Registry, expand government-hosted co-use reading and writing rooms, and continue removing barriers to well-governed Classified Infrastructure-as-a-Service options.
   - DOW modernize SIPRNet provisioning through a unified portal and Service-Level Agreements (SLA), preserve and trust metadata through a Controlled Security Metadata Profile, and reuse standardized cross-domain solution patterns.

4. **Cybersecurity:** Cybersecurity has become the structural constraint of the modern NISP and now functions as the substrate upon which identity, access, telemetry, supply chain transparency, cloud boundaries, data lifecycles, mission continuity, industry participation, and the viability of the acquisition system itself rest, yet oversight is still largely executed using models inherited from physical security. The FAST Study documents 17 recurring cybersecurity challenges, including misaligned System Security Plan (SSP) and inheritance expectations, inconsistent cyber evidence and reciprocity, conflicting Risk Management Framework (RMF) interpretations, unclear shared responsibility models, uniform vulnerability and configuration expectations that ignore cloud, Managed Service Provider (MSP), OT, and legacy constraints, fragmented continuous monitoring, disjointed threat intelligence sharing, and facility-centric cyber models that fail to support emerging mission geographies.



For example, the FAST Study recommends:

- DOW move toward an Integrated Cybersecurity Enterprise Model built on architecture-first oversight, evidence rooted in authentic system behavior and telemetry, uniform and authoritative cross-DOW baselines for cloud, Zero Trust, managed services, OT/ICS, and data lifecycle, and early integration of cybersecurity expectations into acquisition and system design.
- Implement standardized SSP templates and evidence schemas, enforce real reciprocity and shared responsibility, tailor expectations to environment, clarify assessment and change-handling rules, and modernize continuous monitoring and threat intelligence sharing.

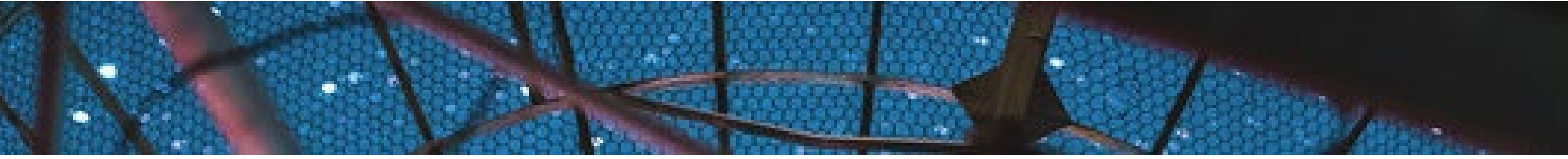
5. **Integration of Security into Acquisition Processes and Contracts:** Acquisition, security, and program offices are not collaborating to the extent necessary, and DOW is missing opportunities to integrate security throughout the acquisition lifecycle in ways that both protect mission and enable speed and innovation. Security personnel and acquisition security professionals are often not involved early in acquisition planning, requirements development, or evaluation; security language in solicitations and contracts can be generic or late; and small businesses and NDCs find complex security requirements fragmented, impenetrable, and costly, which deters entry and encourages overreliance on large primes.

   For example, the FAST Study recommends:

   - OUSW immediately implement cross-functional training and teams that include acquisition security professionals security assessors; require security review and concurrence on acquisition strategies, acquisition plans, statements of work, and solicitations; integrate fit-for-purpose security clauses, performance measures, and evaluation factors into the pre-award phase; and use clear, quantifiable post-award security performance measures and SLAs reinforced by CPARS and incentives to hold contractors accountable for secure deliver.
   - Develop a Small Business Security Roadmap.
   - Provide clearer OTA and CSO security guidance, and streamlined pathways such as FAR Part 12, where appropriate.

Through rigorous data collection and analysis, the MITRE FAST Study demonstrates that acquisition security can be tuned to accelerate delivery, act as a force multiplier for integrity and resilience, and ensure that cost-effective, competitive, and rapid solutions are delivered to the warfighter uncompromised. The most persistent challenges raised across industry were rarely gaps in law or policy. Instead, the challenges emerged mostly from inconsistent implementation, fragmented governance, complexities for NDCs and small businesses, and lack of government compliance with its own processes.

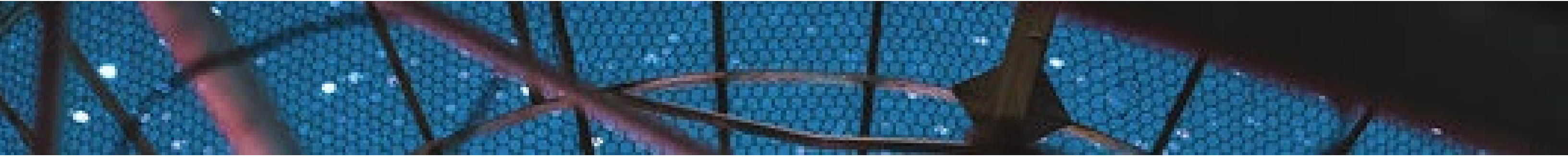
Implementation of the FAST Study's 155 recommended government actions across 63 Security and 11 Acquisition challenges would transform the Department from reactive compliance and fragmented oversight to deliberate security design and unified mission-aligned baselines. With this kind of rapid transformation from industrial security to acquisition security, classified systems and facilities will function as mission-enabling infrastructure, the cleared DIB will broaden through participation of small and nontraditional companies, and warfighters will receive secure capabilities and data at the speed that modern threats demand.



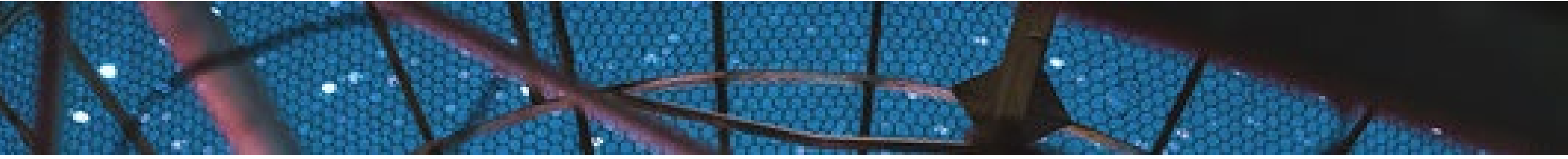
Summary of MITRE FAST Study Challenges and Recommendations

Entity Eligibility and Access

1.	**Lack of DCSA Problem-Solving and Connection to Warfighter Mission Reduces Security Enterprise Urgency**
	Shift mission DCSA mantra from a gatekeeping culture to a warfighter service provider culture, prioritizing connections with the DOW acquisition and mission community and realign central purpose/mission with a more risk-informed approach to safeguard and support the warfighter mission
	Pair DCSA "mission liaisons" with representatives from the MILDEPs or DSEAG with engagement of tactical and operational components to prioritize warfighter needs when DCSA backlogs occur
	Adopt customer-oriented and problem-solving mindset, shifting from rigid "policy will not allow it" response to security enabler approach focused on "how do I enable this securely"
2.	**DCSA Inconsistencies in Guidance and Decisions Delays Projects and Fosters DIB Frustration**
	Address prevailing "checklist mentality" and update internal guidance and training materials to emphasize a risk-based approach
	Institute structured cross-regional program to calibrate interpretations and expectations among ISRs and regional offices, particularly regarding risk-based application of requirements and NISPOM implementation
	Conduct structured review of documentation requirements and process steps, with explicit consideration of risk versus burden
3.	**Facility Clearance Terminology Impedes DIB Entry**
	Issue near-term implementation guidance to deprecate term "Facility Clearance or FCL" and replace it with Entity Clearance
	Remove term Facility Clearance (FCL) from all sections in the rule and other applicable documents and replace it with Entity Clearance (ECL)
4.	**Lack of Entity Clearance Eligibility Sponsorships Creates Barriers to Entry**
	Issue guidance and formalize in a DODI that preparation of DD-254s for classified contract acquisitions be completed no later than solicitation release
	Issue clarifying guidance instructing GCAs to increase direct sponsorship of NDCs, small companies, and medium companies through the Entity Eligibility process
	Study in more detail concerns NDCs, smaller companies, and some government interviewees had regarding prime contractor sponsorship
5.	**Complexity in Preparation of DD Form 254 Hinders DIB Expansion**
	Develop user-friendly DD-254 Preparation Facilitator (PF254)
	Initiate requirements-driven and feedback-driven overhaul of DD-254
6.	**Lack of Automation and Tools Hinders Faster Entity Clearance Package Reviews**
	Employ automation and innovative tools in receipt and initial triage of Entity Eligibility package submissions
	Embrace and support transition of innovative tools to assist companies in completing their Entity Eligibility package
	Engage with DARPA to receive regular updates on TurboFCL prototypes, lessons learned, benefits, and design-phase challenges and to exchange recommendations, common errors, and other challenges observed with Entity Eligibility submissions
	Partner with DARPA or conduct follow-on data collection and analysis to assess impact of TurboFCL and comparable software for preparation of Entity Eligibility package versus manual methods
	Develop standard API to ingest data from any TurboFCL-like solution into NI2
7.	**NISS Change Conditions Cause Holds, Creating Unnecessary Risk**
	Improve efficiency of reviewing and approving change conditions for Entity Eligibility
	Empower DCSA senior regional staff such as regional mission directors and field office chiefs to support review and approval of change conditions
	Treat NI2 as fundamental modernization of NISS and not incremental patch to align system with needs of modern DIB

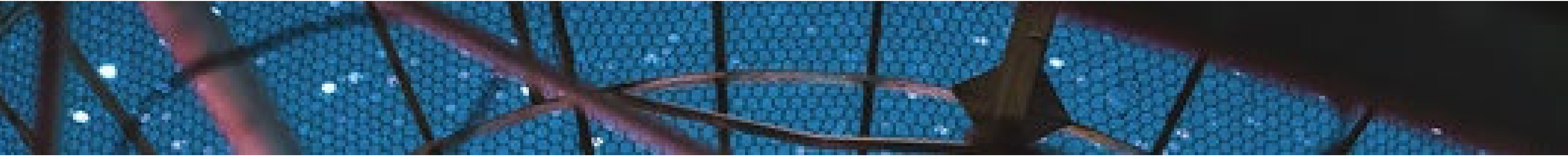


	Re-prioritize implementation of complete NI2 to 2026
8.	**Outdated Facility Clearance Orientation Handbook Increases Subcontractor Confusion**
	Update and expand Facility Clearance Orientation Handbook, rename as Entity Clearance Orientation Handbook, and update related documentation to simplify processes and improve transparency
	Update Handbook within six months of receiving FAST Study report
9.	**DOD Enhanced Security Program (DESP) Underutilization Reduces Innovative Problem-Solving**
	Extend DESP to Top Secret level information and announce change broadly including at NISPPAC
	Issue implementation guidance allowing companies to use DESP for small number of technical experts and business development staff to review and respond to classified solicitations prior to their company being sponsored for Entity Eligibility
10.	**Lack of Co-Use Spaces for Classified Proposal Development Restricts Competition**
	Increase funding for and availability of government-hosted classified proposal reading and writing rooms
	Develop and adopt standardized DOW-wide co-use template to streamline processes
	Approve secure sites as co-use spaces by default
	Provide access to all classified DOW RFPs and RFIs in one platform when possible
	Advocate for and remove barriers to consider Classified-Infrastructure-as-a-Service (CIaaS) providers
11.	**Cybersecurity is Not a Required Key Management Personnel Role, Leading to Systemic Risk**
	Issue implementation guidance that DIB companies yet to start Entity Eligibility Determination process will include ISSM as required fourth KMP
	Require companies already possessing Entity Eligibility to attest and name cleared individual performing ISSM KMP role
12.	**Government-Administered SCI Indoctrination Diminishes Project Cost and Efficiency**
	Issue guidance allowing trusted DIB companies with proven security records to conduct classified indoctrination briefings for company and subcontractor employees approved for project-specific cleared access
13.	**Prolonged Delays for Additional Entity Clearances Reduces Availability of Classified Facilities**
	Issue implementation guidance allowing trusted DIB companies with proven security records to self-certify additional company sites for Entity Clearance Eligibility
	Conduct audit of self-assessed site for Final Entity Clearance Eligibility within two years
14.	**Limited Access to SCI and SAP Slots Creates Workarounds**
	Adopt risk-based approach to SCI and SAP "read-on" slot allocation, moving from rigid slot caps system to framework that balances mission need, operational continuity, and security risk
	Update DODM 5105.21 to incorporate risk-based approaches for SCI and SAP "read-on" slot allocation
	Address limitations in allocated PCL slots, particularly for corporate overhead staff, via updates to Volume 3 of DODM 5105.21
15.	**Lack of Personnel Clearance Reciprocity Increases Cost and Delays DIB Support to Warfighter**
	Accept reciprocity in PCLs across DOW as requirement for mission success and enforce it using existing authorities and reforms underway through TW 2.0
	Establish single, integrated framework for PCLs and adjudications that all IC and DOW components are required to follow
	Harmonize polygraph procedures including formats, quality control, and handling of inconclusive results
	Treat PCL-eligibility as shared, government wide decision
	Recognize training completed for another agency where content and frequency are effectively the same and align reporting obligations such as foreign travel or foreign contact reporting
16.	**Terminology Ambiguity in Personnel Clearances (PCL) Reduces Onboarding Readiness**
	Issue guidance that term PCL must be used in conjunction with terms Eligibility or Access in future to designate individual national security clearance status and specify enrollment in CV
17.	**Misaligned Entity and Personnel Clearance Eligibility Timeframes Reduce DIB Availability**
	Develop and release clarifying guidance specifying PCL Eligibility and Entity Eligibility will require full background investigation after five years' break in service
18.	**Conflation of National Security and Suitability/Fitness Adjudications Impedes Reciprocity**
	Disaggregate national security clearance adjudication from position adjudication for DOW military, civilian, and contractor personnel



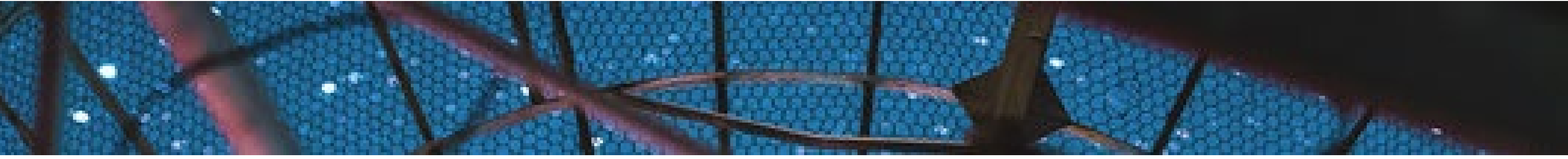
Foreign Ownership, Control, or Influence (FOCI)

19.	**SF-328 Complexity and Inefficient Review Process**
	Implement more efficient automated error check to triage SF-328 information
	Prioritize continuous evaluation and improvement of SF-328 reviews to ensure efficiency and effectiveness
20.	**Understanding the New SF-328**
	Continue to collaborate closely with industry to ensure SF-328 terminology is consistent with common business terminology
	Provide additional guidance on new SF-328, clarifying what levels to document within supply chains and investments, and defining "material change" within those levels
	Provide DCSA staff with education and training on modern ownership models, VC models, diluted versus outstanding investments, investment structures, private equity structures, seed investors, and cap tables
21.	**Negative Perceptions of FOCI-Mitigated Companies**
	Issue Directive-Type Memorandum clarifying that SF-328 is only ever sent directly to DCSA, prohibiting inclusion in solicitation documentation, and promoting acquisition officials coordination of FOCI questions directly with DCSA rather than with industry
	Consider approved FOCI mitigation plans and companies security ratings when making award decisions rather than simply presence or absence of FOCI to prevent exclusion of FOCI-mitigated companies
	Update acquisition officials' source selection training to improve understanding of FOCI and mitigations
22.	**Delays in Finalized FOCI Mitigation Agreements**
	Eliminate delays in finalizing negotiated agreements by requiring more rapid DCSA final signatures and approval processing
23.	**Ineffective Use of Outside Directors and Government Security Committees**
	Process administrative changes faster
	Integrate business terminology into mitigation documentation and OD/PH training so companies can more quickly and accurately understand mitigation implementation and business impacts
	Conduct more regional and individual meetings with ODs to facilitate direct engagement
	Leverage ODs better by identifying areas for immediate change in authorities to make decisions without DCSA approval and rely on ODs to exercise discretion in wider range of decisions
24.	**Need for Modernized Electronic Communications Plans (ECP)**
	Focus technology protections on technology transfer and anti-tampering monitoring to gain more confidence from DOW customers in FOCI-mitigated companies
25.	**Burdensome Affiliated Operations Plan (AOP)**
	Build "playbook" or collection of mitigations, governance techniques, and controls for various shared services based on risk, and promote baseline mitigations to reduce overall and redundant content
26.	**Outdated Templates and Guides**
	Update TCP template and AOP guide and produce guidance for TCP and ECP
27.	**Duplication Between ECP and CMMC**
	Reuse validated CMMC Level 2 artifacts for ECP's overlapping cyber controls and reduce ECP scope to areas not covered by CMMC
28.	**NDAA Section 847 $5M Threshold Remains Undefined**
	Describe clearly how "exceeding $5M" will be defined and implemented
29.	**NDAA Section 847 Implementation Guidance Woefully Needed**
	Increase awareness through education and outreach to better prepare industry for Section 847
	Consider existing cleared entities, including FOCI-mitigated companies, with an Entity Eligibility in good standing as already qualified under Section 847
	Develop structured reviews of SF-328 to enable regional and field officers to determine when there is no need for further FOCI review or mitigation
	Provide implementation guidance on timing and process of flowing 847 requirements between acquisition offices, prime contractors, subcontractors, and DCSA
30.	**Current FOCI Approach is Outdated**
	Fund comprehensive study to evaluate DCSA's current approach to FOCI, including return-on-investment of current review and mitigation approaches and potential data-driven modifications



Safeguarding of Classified and Sensitive Information

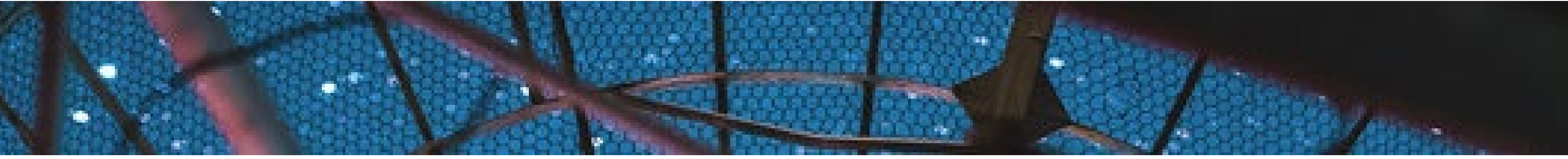
31.	**Programs Begin Without CPI, CTI, CUI and Fail to Establish Early, Authoritative Protection Plans**
	Establish mandatory Program Protection Baseline (PPB) as acquisition gating artifact
	Require acquisition and contract mechanisms that formally recognize PPB, PPP, SCG, and authorized CUI guidance as Government-furnished prerequisites upon which contractor performance, compliance, and delivery timelines depend
	Ensure timely execution-phase delivery and flowdown of approved protection artifacts
	Require applied, role-specific CUI training for government enabling consistent execution of authoritative CUI policy across acquisition, security, engineering, and program management
32.	**CUI Policy Implemented Inconsistently Across DOW**
	Issue binding Department-level policy instrument that mandates single, authoritative CUI Marking and Dissemination Profile applicable across all MILDEPs
	Enforce use of authoritative CUI profile through acquisition entry points
	Operate Department-wide mechanism to identify, adjudicate, and correct government-side CUI mislabeling and mishandling; advocate for government-wide directive that establishes parallel obligations, reporting, and consequences for government personnel handling of CUI
33.	**Lack of Standardized and Practical CUI Training Risks Mishandling**
	Establish standardized, mandatory CUI training baseline for industry
34.	**New Entrants and Subcontractors Face Reduced and Unpredictable Access to Classified Space**
	Require programs and primes to develop and maintain classified facility access plans for subcontractors
35.	**SCIF Accreditation Timelines Are Unreasonable**
	Finalize DIA responsibility long-term, and fully staff accreditation office with improved throughput by temporarily assigning MILDEP staff skilled at accreditation while hiring
	Implement time-bound accreditation milestones and require DIA to publish regional performance metrics
	Require government programs to incorporate SCIF planning earlier in acquisition process and coordinate with DIA before contract award to validate feasibility
36.	**DOW SCIF Reciprocity Exists in Policy but Fails in Practice**
	Issue Department-level memorandum reaffirming and enforcing DOW SCIF reciprocity as default expectation across all MILDEPs and regions ('a SCIF is a SCIF' in DOW)
	Issue guidance explicitly stating that effective SCIF reciprocity is prerequisite for success of Classified Infrastructure-as-a-Service (CIaaS) models
	Establish secure, Department-wide catalog of accredited SCIFs and other classified facilities
	Formalize additional category of accredited classified facilities designated as Enterprise DOW SCIFs
37.	**Underuse of Co-Use Agreements Forces Redundancy and Underutilization**
	Issue guidance establishing co-use of existing accredited classified space as default operating model (justification requirement if co-use denied)
	Publish uniform criteria for acceptable co-use arrangements and provide advisory support to programs evaluating shared infrastructure options
38.	**Mandatory Replacement of "Black-Label" Security Containers Imposes High Cost for Perceived Marginal Security Benefit**
	Adopt risk-based approach to "black-label" security container phase-out that allows continued use where containers are demonstrably functional and deployed within environments with security-in-depth measures
39.	**SIPRNet Provisioning Is Slow, Opaque, Regionally Inconsistent, and Constrained by Outdated Filtering Models**
	Develop enterprise SIPRNet provisioning portal that unifies submission, tracking, adjudication, and escalation across DISA, DCSA, and MILDEPs
40.	**Classified Cloud Adoption Is Impeded by Redundant Information Owner Approval Requirements**
	Issue implementation guidance clarifying information owner approval requirements in DFARS 252.239-7009 and 252.239-7010 do not apply to classified cloud environments authorized by DCSA and DISA
41.	**Metadata Is Not Preserved or Trusted Across Systems, Preventing Reliable Marking and Cross-Domain Movement**



	Produce Controlled Security Metadata Profile (CSMP) as authoritative, mandatory schema for all classification markings, CUI categories, dissemination rules, provenance, and automated enforcement
42.	**Cross-Domain Solution Rebuilds Delay Mission Execution and Produce Conflicting Approval Outcomes**
	Sponsor and maintain Department-recognized library of reusable CDS patterns
43.	**Small Businesses and NDCs Find Complex Security Requirements Impenetrable and Costly**
	Fund, advocate for, and promote specific scalable initiatives that translate security requirements into operational practices and share leading security practices with small businesses and NDCs
44.	**DOW Programs Cite Outdated or Superseded Policy Causing Delays or Rework**
	Create and maintain single authoritative, version-controlled repository containing canonical URLs for all relevant security, classification, CUI, cybersecurity, RMF, and program protection policy
45.	**Overlapping Roles Between DOW CIO, OUSW(I&S), OUSW(A&S), and OUSW(R&E) Cause Divergent Instructions**
	Develop formal, published RACI matrix defining roles, responsibilities, and decision rights of DOW CIO, I&S, A&S, and R&E for classification, CUI, program protection, cybersecurity, and IT requirements
	Implement time-bound adjudication mechanism programs can invoke whenever directives from DOW CIO, I&S, A&S, and R&E conflict
46.	**Regional Variation in DCSA Interpretations Burdens Industry**
	Reemphasize mandated uniform training for DCSA inspectors, require cross-regional calibration reviews, and implement enterprise-wide quality control mechanisms
	Publish anonymized metrics revealing regional variations for oversight and continuous improvement
	Implement centralized adjudication mechanism when regional interpretations conflict

Cybersecurity

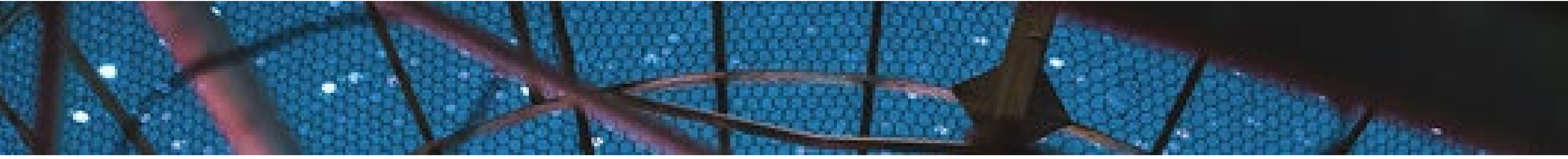
47.	**Misaligned System Security Plans and Inheritance Expectations Drive Rework and Reviewer Disagreement**
	Mandate standardized SSP template aligned to cloud, MSP, OT, and hybrid architectures that clearly distinguishes contractor-owned controls from inherited controls
48.	**Inconsistent Cyber Evidence and Reciprocity Undermine Predictable Authorization Outcomes**
	Implement mandatory, authoritative cyber evidence schema that defines acceptable artifacts for cloud-native, MSP-managed, hybrid, and on-premises systems
49.	**Conflicting RMF Interpretations Create Excessive Documentation with Limited Security Value**
	Define authoritative minimum RMF documentation standard and clear limits on expansion beyond it, emphasizing risk relevance, architecture, inheritance, and continuous monitoring outcomes
50.	**Unclear Shared Responsibility Models Leave Critical Cyber Controls Unowned**
	Publish unified shared-responsibility model covering cloud, MSP, hybrid, and OT-adjacent environments, with inheritance matrices defining ownership of security controls including ICAM and access enforcement
51.	**Cyber Reciprocity Failures Force Re-authorization of Identical Architectures**
	Enforce reciprocal acceptance of validated cyber authorizations and evidence across regions and MILDEPs through enterprise-level governance
52.	**Inconsistent Cybersecurity Assessment Execution and Change Handling Undermine Security Outcomes, Cost, and Industrial Base Stability**
	Establish authoritative, enterprise-level governance for cybersecurity assessment execution and change handling, while preserving MILDEP authority for mission risk acceptance
53.	**Variable Cloud Architecture Evaluations Block Standardized Authorization Paths**
	Define authoritative ZTA and ICAM baselines mapped to common cloud and hybrid architecture patterns
54.	**Uniform Vulnerability Management Expectations Ignore Cloud, MSP, OT, and Legacy Constraints**
	Implement environment-aware vulnerability management framework differentiating expectations for cloud and SaaS, MSP-managed infrastructure, OT and ICSs, and legacy or vendor-controlled systems
55.	**Inconsistent CUI and Sensitive Data Governance Breaks Lifecycle Protection across Modern Toolchains**
	Define authoritative CUI data lifecycle model that governs data from origination to final disposition



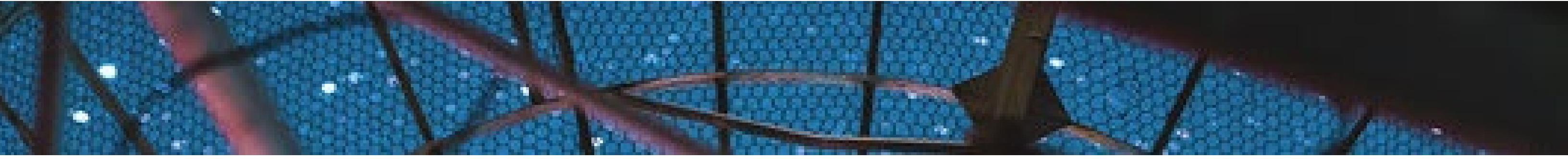
56.	**Fragmented Continuous Monitoring Expectations Prevent Comparable Cyber Risk Decisions**
	Implement architecture-aware continuous monitoring standard that defines acceptable telemetry sources, reporting mechanisms, and escalation paths across cloud, MSP, OT, and legacy environments
57.	**Undefined OT Cyber Requirements Disrupt Operations without Improving Security Outcomes**
	Define and implement distinct OT cybersecurity evaluation framework that recognizes stability and availability as core security properties
58.	**Misaligned Logging and Audit Expectations Exceed Capabilities of Cloud, MSP, OT, and Legacy Systems**
	Implement standardized, outcome-oriented telemetry and logging requirements aligned to threat detection, incident response, and mission impact
59.	**Configuration Management Requirements Conflict with Provider-Managed and OT Environments**
	Develop environment-aware configuration management framework that defines how configuration responsibilities and expectations map across cloud, MSP, OT, and legacy systems
60.	**RMF Processes Fail to Align with Modern, Distributed Architectures**
	Implement mandatory, repeatable mechanism requiring cybersecurity architectures and RMF baselines to be explicitly derived from Program Protection Baseline
61.	**Fragmented System Boundary Definitions Produce Conflicting Cyber Requirements for Identical Architectures**
	Define and enforce unified boundary determination framework aligned to modern architectures and Zero Trust principles
62.	**Disjointed Threat Intelligence Sharing Limits Collective Defense Across the DIB**
	Implement enterprise-wide, repeatable model for delivering actionable cyber threat intelligence across DIB
63.	**Facility-Centric Cyber Models Fail to Support Emerging Mission Geographies**
	Implement governance model that treats emerging mission geographies as first-class operational constructs rather than exceptions to legacy facility frameworks

Integration of Security into Acquisition Processes and Contracts

64.	**Acquisition Workforce**
	Ensure DOW has qualified staff to achieve security integration throughout the acquisition lifecycle
	Meet requirements of an acquisition security training and credentialing program developed in accordance with DODM 3305.13 and the guidance in this issuance
	Conduct security reviews of contracts, agreements, and other acquisition-related documents to ensure they meet the required security standards
	Provide security training and awareness to program managers, engineers, contractors, and stakeholders to ensure they understand security risks associated with acquisition process and steps to mitigate those risks
	Use training and education, security toolkits and reference materials, role-based integration, routine security reviews, and collaborative culture to foster stronger security awareness at all acquisition stages
65.	**Integration of Security Throughout the Acquisition Process**
	Use Cross-Functional Training (CFTs) throughout acquisition lifecycle, and then cross-functional teaming
	Ensure acquisition strategies and plans obtain security review and concurrence or approval
	Ensure security is involved during requirements development, Work Statement drafting, and relevant security-related performance measures
	Assist with drafting security-related instructions to offerors and evaluation factors/criteria so offerors are required to propose their approach to security in technical/security proposals and price/cost proposals
	Review RFPs/solicitations and contracts prior to issuance to ensure required/desired security language is complete and accurate
	Include security as members of proposal evaluation team in some capacity (e.g., voting member or advisor) based on acquisition and evaluation factors or volume structure
66.	**Collaborative Requirement Development (Pre-Award)**
	Create CFTs and, if needed, integrated project teams (IPTs) with members from security, program, and contracting offices to validate and prioritize security requirements



	Require unified planning across security domains so security offices and acquisition security professionals assess risks, develop unified requirements, and draft or provide input into security language covering information, systems, personnel, and facilities
	Integrate acquisition security professionals into requirements, work statement, and solicitation drafting
	Define what requires protection, how much protection is necessary, and duration of protection
67.	**Inclusion of Security Clauses (Pre-Award)**
	Ensure all solicitations require compliance with mandated security frameworks (e.g., NISPOM for classified programs, DFARS for cybersecurity, Physical Security standards)
	Mandate use of DD-254 for classified contracts, specifying facility and personnel security requirements
68.	**Acquisition Strategy and Planning (Pre-Award)**
	Add signature blocks for acquisition security professional and security organization(s) to concur or approve Acquisition Strategy and Acquisition Plan
	Hold industry days or Q&A sessions that include federal and industry security experts to ensure security requirements are properly included in acquisition documents
	Issue RFIs to request input on security requirements to ensure properly included in acquisition documents
69.	**Proposal Evaluation (Pre-Award)**
	Incorporate non-price factors into evaluation that encourage new entrants and smaller businesses, and foster security planning
	Evaluate offeror’s experience, past performance, qualifications and certifications of key personnel in security roles, and technical or management approach to maintaining security, incident response, and reporting as described in the solicitation
	Treat physical, personnel, and cybersecurity as distinct technical evaluation elements (not ‘compliance’)
70.	**Formal Performance Measures and SLAs (Post-Award)**
	Include Service Level Agreements with quantifiable thresholds for security (e.g., % of vulnerabilities remediated within timeframe, background check completion rates, physical access control compliance)
	Define how metrics will be monitored and enforced (penalties, service credits, corrective action plans) or rewarded (especially with incentive type contract)
	Structure performance measures/evaluations around key milestones and contract closeout, documenting contractor performance on security
71.	**Program Offices Holding Contractors Accountable (Post-Award)**
	Provide program managers and CORs with acquisition security professional support and CDSE training to help with post-award security oversight responsibilities
	Require regular reporting and deliverables on security posture reports, incident logs, clearance status
	Schedule and document regular compliance reviews, penetration tests, and site visits
	Establish clear escalation paths for reporting and remediating non-compliance with security requirements
72.	**Integrated Oversight and Communication (Post-Award)**
	Maintain active communication and information-sharing between program, security, and contracting offices during contract execution
	Use contract management tools to track compliance with security requirements across stakeholders
73.	**Subcontractor Management (Post-Award)**
	Ensure prime contractors flow all required security clauses down to subcontractors and check compliance, including reporting and controls for classified work or CUI
	Require offerors to indicate their procedures for ensuring subcontractor compliance to security requirements to include any flowdown of clauses
74.	**Contract Close-out Requirements (Close-Out)**
	Follow current close-out requirements and reference DOD’s 2019 Contract Closeout Guide Book or revise if needed to implement DOW SecWar strategy
	Utilize contract close-out security checklists, such as DD Form 1597, to verify disposition of classified material (confirm through DCSA and annotate), patents, royalties, and proper reporting
	Include contractor close-out requirements as needed in PWS to ensure contractor is aware of and bound to its contract close-out requirements
	Conduct lessons learned involving acquisition/contracting offices, security offices, and program offices to improve future contract security integration and update processes in DOD’s Contract Closeout Guide Book



1. BACKGROUND AND PURPOSE

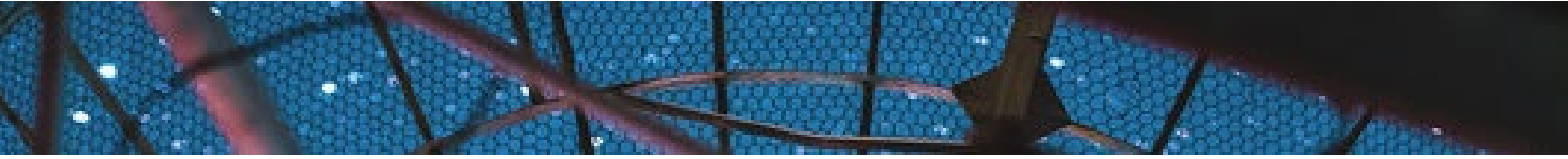
The Department of War (DOW) is undertaking once-in-a-generation acquisition reforms, emphasizing contracting speed, flexibility, and rapid delivery. Any effort to reform DOW acquisitions cannot be successful without also addressing unnecessarily burdensome and outdated security processes. Sponsored by the Office of the Under Secretary of War for Intelligence & Security (OUSW(I&S)), MITRE's Fast-tracking Acquisition Security Transformation (FAST) Study is a targeted, systematic, deep-dive analysis to pinpoint and prioritize challenge areas in DOW security requirements, policies, and practices that unjustifiably impact cost, schedule, and performance. Between May and December 2025, the MITRE FAST Study team collected and analyzed data, then identified specific, measurable recommended government actions to advance our warfighters by modernizing critical security requirements and processes for greater effectiveness and efficiency. Ultimately, MITRE's FAST Study aims to advance usable, effective security to support the Secretary of War's (SecWar) and the Department's goals of strengthening and protecting our warfighters and expanding the Defense Industrial Base (DIB).

The MITRE FAST Study proceeds from an articulated *acquisition security* definition: "The proactive planning and integration of all security disciplines and other defensive methods into the defense acquisition process to protect weapons systems and related sensitive technology; technical information such as research data with military applications; and support systems from foreign intelligence collection, unauthorized disclosure, sabotage, theft, or damage throughout the technology's life cycle." (DOW Defense Acquisition University, 2025). The definition is a guidepost for ensuring security truly enables, not hinders, rapid and secure delivery.

The premise of the FAST Study is that the National Industrial Security Program (NISP), established by Executive Order 12829 in January 1993, was designed for a vastly different era of DOW acquisition practices, systems, DIB, and threat environment. In the intervening 32 years, little has changed in the NISP's overall framework. Now is the time to optimize the DOW's acquisition security approach, whether through NISP, Controlled Unclassified Information (CUI), or other security requirements, to effectively support rapid acquisition reform and strengthen the security posture protecting all warfighter capabilities.

The Department's broader *Acquisition Transformation Strategy: Rebuilding the Arsenal of Freedom (2025)*[1] (hereafter referred to as DATS) prioritizes speed, flexibility, and rigorous execution and places the acquisition system and industrial base on a wartime footing. The SecWar has directed the DOW to accept more risk in the Warfighting Acquisition System (WAS), transitioning from a culture of compliance to one of speed and execution, while rapidly tackling strategic challenges. The FAST Study is intentionally aligned with these outcomes and pillars because acquisition security must enable and accelerate these objectives. For example, maximizing flexible contracting, digitizing acquisition, and using portfolio scorecards will benefit from security requirements that are fit-for-purpose, consistent, and implementable with speed and

[1] DOW (2025). *Acquisition Transformation Strategy: Rebuilding the Arsenal of Freedom*. Source: https://media.defense.gov/2025/Nov/10/2003819441/-1/-1/1/ACQUISITION-TRANSFORMATION-STRATEGY.PDF



precision across the enterprise. These same reforms advance the President's Management Agenda[2] priority to "buy as one entity—smarter, faster, cheaper" by aligning security implementation with the agenda's plan for an agile, efficient procurement system.

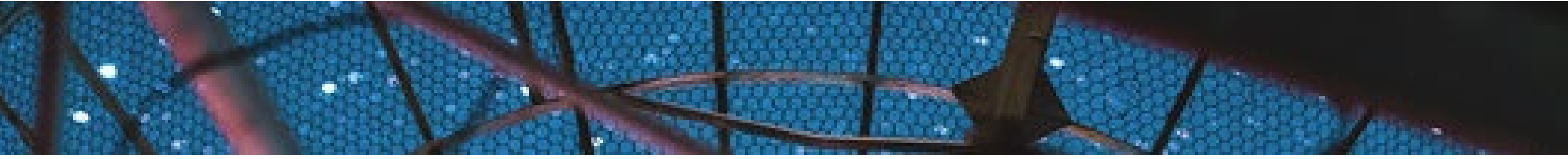
In May 2025, OUSW(I&S) tasked MITRE to analyze opportunities that optimize acquisition security to more quickly and securely enable the DIB to put key technologies in the hands of our nation's warfighters and not our nation's adversaries. MITRE collected data through interviews, questionnaires, and focus groups representing 6,734 security industry leaders, practitioners, and innovators from 105 organizations across the DIB. These organizations included 65 small, medium, and large businesses; five nontraditional defense contractors (NDCs); 19 Security-as-a-Service providers; and 14 industry councils and consortiums. MITRE's experienced behavioral sciences and security practitioners applied systematic quantitative and qualitative data analysis techniques to identify patterns in industry's challenges, which were then validated with external or government data where available and accessible. For example, the team triangulated challenges using government policy, process, and implementation guidance to ensure recommended government actions for change were practical and grounded in government data wherever possible.

Data collection was designed to identify specific government security policy, process, and practice challenges that adversely impact cost, schedule, and performance when working (or trying to work) with the DOW. The FAST Study focused on specific areas of DOW acquisition security requirements, practices, and systems outlined in the following Methodology section. Example focus areas included Facility Clearances, Foreign Ownership, Control, or Influence (FOCI), Classified Facility Accreditation, Information System Authorizations, and Cybersecurity.

As Department policy is designed to be flexible, clarifying policy requirements using implementation guidance is central to accelerating acquisition security. Whereas most other Cognizant Security Agencies (CSAs) can design and optimize security implementation for a single organization, the uniform "one-size-fits-all" security approach does not apply to DOW. Throughout data collection and analysis, a recurring friction was identified: Defense Counterintelligence and Security Agency (DCSA) personnel have too much discretion in interpreting and applying security rules as self-described gatekeepers. Some security decisions were discretionary and some people in those roles made certain decisions discretionary. The result is inconsistent implementation between policy frameworks, fragmented interpretations, frustration across industry, and unpredictable timelines for clearances, facility accreditation, and system authorizations that build on already inconsistent interpretations between Military Departments (MILDEPs). Consequently, the FAST Study's recommended government actions emphasize consistency, reciprocity, and pragmatic application at enterprise scale, empowering the security apparatus to more reliably move with speed and rigor.

The FAST Study also addresses today's business realities, which shape access to controlled information and classified work. Recommendations for government action heavily consider how companies think about entering the DIB or scaling involvement with the DOW. Companies seeking to contract directly with the DOW need adequate security leadership and capabilities.

[2] Executive Office of the President (2025). *President's Management Agenda*. Source: https://www.performance.gov/pma/

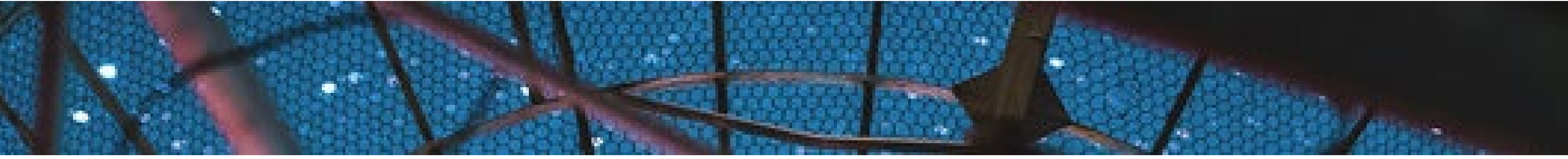


If investing in advance of DOW contracts to grow their defense business is too onerous or not aligned with company leadership priorities, then partnering as a subcontractor to a DIB prime contractor company is the appropriate path to gain access, learn requirements, and build capabilities incrementally. Critical levers to more efficiently and securely enable new entrants as subcontractors include incentivizing DIB prime contractors to sponsor more small or medium-sized businesses (SMBs) and NDCs for entity clearance eligibility, and improve the DIB's ability to pass classification guidance and program protection plans downstream to subcontractors.

The FAST Study was conducted against the backdrop of Executive Order 14265 ("Modernizing Defense Acquisitions and Spurring Innovation in the Defense Industrial Base")[3] and complementary Department initiatives to modernize and rapidly reform defense acquisitions. The Executive Order presents a unique opportunity to clarify or modify security requirements and processes to remove barriers, cancel burdensome or out-of-date requirements, update requirements and policies that have fallen behind emergent threats, accelerate deployment of emerging technologies to maintain military superiority, and keep government accountable by ensuring security requirements and processes are justified, measurable, and fit-for-purpose. MITRE's data collection and analytic approach was explicitly designed to support these priorities by identifying options to accelerate acquisition security processes in support of broader acquisition transformation. This approach will assist Program Executive Officers (PEOs) and Program Acquisition Executives (PAEs) in making decisions with speed. With consistent, rationalized, and implementable security requirements, Program Managers (PMs) can tailor processes and allocate funds with agility, and industry can invest with confidence.

Ultimately, through this OUSW(I&S)-funded FAST Study, MITRE identified government security requirements—whether owned by OUSW(I&S) or not—that should be clarified, modified, or cancelled to advance secure delivery at the rapid speed needed for warfighters to successfully fulfill mission requirements. By integrating security into acquisitions in ways that are usable and effective, the Department can rebuild the Arsenal of Freedom while protecting the sensitive technologies that give our warfighters decisive advantage.

[3] The White House (2025). *Modernizing Defense Acquisitions and Spurring Innovation in the Defense Industrial Base.* Source: https://www.whitehouse.gov/presidential-actions/2025/04/modernizing-defense-acquisitions-and-spurring-innovation-in-the-defense-industrial-base/



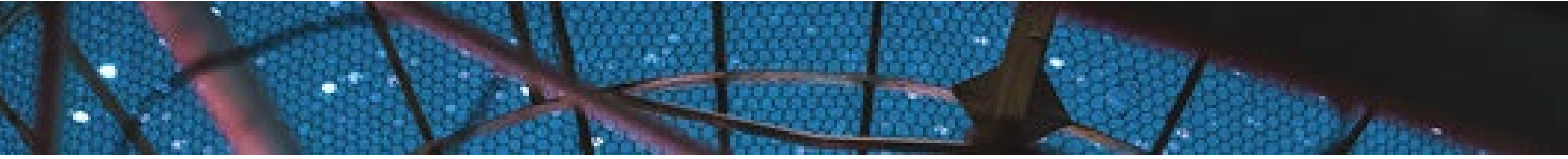
2. METHODOLOGY

The FAST Study was designed as a targeted, systematic, deep-dive data collection and analysis of government security requirements, practices, and systems that impact the ability of the DIB to quickly, affordably, and successfully enable the warfighter mission. The FAST Study team analyzed quantitative and qualitative data collected from structured interviews, questionnaires, and focus groups with 6,734 industry organizations across the DIB, supplemented by focused expertise and experience by MITRE behavioral sciences and security researchers, practitioners, and subject-matter-experts. Table 1 provides a breakdown of the industry organizations that participated in the FAST Study. To maximize industry candor, all interviews, questionnaires, and focus groups were treated as non-attributable. This was necessary because some companies described fear of losing contracts or relationships they spent years building if they shared problems with government or prime contractors. For example, one industry interviewee described "gate-keeping and retribution is real with primes" and government or prime contractors can state "I will go a different direction" to close discussions with no-accountability or company recourse. The collected data was recorded using anonymous interviewee numbers, de-identified to the extent possible, and access restricted to only the MITRE FAST Study team; no government employees, industry organizations, or other MITRE teams have access to participating industry data.

Table 1. FAST Study Industry Sample

Industry Type	Number
Defense Contractors	65
• Small Businesses	28
• Medium-sized Businesses	7
• Large-sized Business	18
• Academic Institutions	12
NDCs	5
Security-as-a-Service Providers	21 (representing 3269 industry companies)
Council/Consortiums	14 (representing 3360 industry companies)

For the interviews, questionnaires, and focus groups, MITRE adopted a sampling strategy reflecting the diversity of industry companies engaged in DOW acquisitions, the practical pathways in which capabilities enter and scale within the DIB, and the DOW's goals for expanding the DIB. MITRE centered data collection on **defense contractors** which are organizations with or recently had contracts with the DOW, including four key types:



- **Small businesses:** Businesses which do not exceed the size standard for the North American Industry Classification Systems (NAICS) code that best describes the product or service being offered by the business to the government.[4]
- **Medium-sized businesses:** Businesses with revenue or employees up to five times above the Small Business Administration (SBA) small size standard.[5] Generally, these businesses had more than 500 but fewer than 1,000 employees or revenue between $10 million and $1 billion.[6]
- **Large businesses**: Businesses with revenue or employees exceeding five times the SBA small size standard were classified as large.[7] Generally, these businesses had more than 1,000 employees and were competing for multiple government contracts.
- **Academic institutions:** Universities and colleges performing DOW-funded basic and applied research.

MITRE tried to engage NDCs**,** which refers to organizations not currently performing and have not performed any contract or subcontract for the DOW in the last year.[8] NDCs included startup businesses pursuing or planning to pursue DOW work but had not yet received an award. Engaging NDCs proved challenging because many are not presently seeking DOW work; therefore, they were reluctant or did not see benefit in participating in the FAST Study. As a result, data was collected from a limited number of NDCs and is included in this report, although proportionally smaller than other industry types.

In addition to defense contractors and NDCs, MITRE engaged two other key industry types critical within the DIB:

- **Security-as-a-Service Providers:** Companies that provide advice, consultancy, products, or services enabling other companies to meet government security requirements. Advisory or consultancy services include entity eligibility, FOCI, Facility Security Officers (FSOs), cybersecurity, and classified facilities accreditation amongst others. Operational products and services include providing associate Facility Security Officers (FSOs), access to classified facilities and information networks, and third-party assessments (e.g., Cybersecurity Maturity Model Certification (CMMC) Third-Party Assessment Organization (C3PAOs)).
- **Councils and Consortiums:** Organizations that convene cross-government/industry working groups, provide industry representation and guidance to government, and disseminate practices and implementation artifacts to industry members. Representative bodies included NISP Policy Advisory Committee (NISPPAC), Academic Security and Counter Exploitation

[4] SBA (2023). *Table of Size Standards*. Source: https://www.sba.gov/document/support--table-size-standards

[5] GAO (2019). GAO-19-523: *Federal Contracting: Awards to Mid-Sized Businesses and Options for Increasing Their Opportunities (p. 13)*. Source: https://www.gao.gov/assets/gao-19-523.pdf

[6] National Center for the Middle Market (2025). *Information Sheet.* Source: https://www.middlemarketcenter.org/Media/Documents/NCMM%20InfoSheet.pdf

[7] GAO (2019). GAO-19-523: *Federal Contracting: Awards to Mid-Sized Businesses and Options for Increasing Their Opportunities (p. 13)*. Source: https://www.gao.gov/assets/gao-19-523.pdf

[8] The NDC definition is a simplified version of the full definition outlined in 10 U.S. Code § 3014, specifically "entity that is not currently performing and has not performed, for at least the one-year period preceding the solicitation of sources by the Department of Defense for the procurement or transaction, any contract or subcontract for the Department of Defense that is subject to full coverage under the cost accounting standards prescribed pursuant to section 1502 of title 41 and the regulations implementing such section.." Source: https://www.govinfo.gov/content/pkg/USCODE-2024-title10/pdf/USCODE-2024-title10-subtitleA-partV-subpartA-chap201-subchapII-sec3014.pdf

(ASCE), Armed Forces Communications and Electronics Association (AFCEA), Community Association for Information System Security Working Group (CAISSWG), Industrial Security Working Group (ISWG), Intelligence and National Security Alliance (INSA), and National Defense Industrial Association (NDIA). Additional councils and consortiums were invited to participate on multiple occasions but did not respond during the FAST Study period.

In addition to direct reach out to companies and organizations, the MITRE team leveraged outreach channels including in-person and virtual government and industry hosted conferences and industry days; coordination with MILDEPs and other U.S. Government (USG) agencies (e.g., Federal Bureau of Investigations (FBI) Private Sector Coordinators); collaboration with DOW small business programs (e.g., DOW Office of Small Business Programs, SBIR/STTR Program); and engagement with councils and consortiums, venture capital investment companies, and regional innovation hubs. The FAST Study team appreciates these partners for circulating invitations and promoting engagement with their membership, significantly expanding data collection.

The FAST Study team prioritized industry-facing data collection in line with its goal of emphasizing industry challenges from the perspective of industry companies, rather than relying on government interviews or internal government documents. Where necessary to contextualize specific data, the FAST Study team conducted a limited number of interviews with government leaders and reviewed publicly available policy and guidance. Relevant policy and guidance included:

- Title 32 of the Code of Federal Regulations (CFR) Part 117 (NISP Operating Manual (NISPOM))
- Federal Acquisition Regulation (FAR)
- Defense Federal Acquisition Regulation Supplement (DFARS)
- Office of Inspector General (OIG) reports
- DOD Directives (DODD), Instructions (DODI), Manuals (DODM), and Memorandums

Formal document requests for standard operating procedures, concepts of operations, delegation memoranda, interim materials, or other pre-decisional drafts were not pursued. A USG shutdown during the FAST Study resulted in some government websites and repositories being unavailable, which reinforced the decision to work primarily from industry-provided inputs and publicly available sources. This design ensures recommended options are justified by open evidence and implementable across MILDEPs without dependence on restricted content, as well as preserving transparency, reproducibility, and scientific rigor.

SCOPE

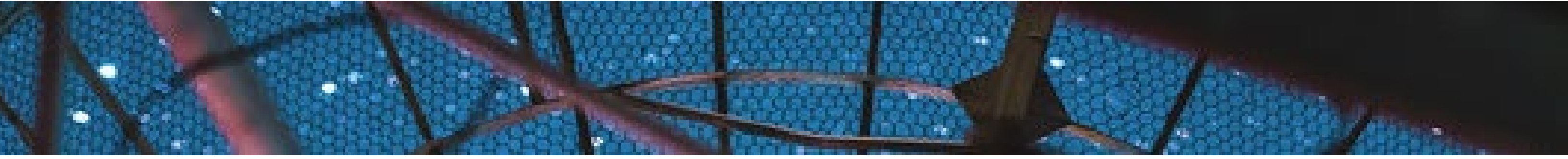
The FAST Study centered on five key focus areas. Acquisition security focus areas were selected based on their direct relevance to industry's ability to compete for and execute on DOW contracts, and feasibility of collecting industry data within the FAST Study's five-month industry engagement timeframe (July to November 2025). The focus areas were approved by OUSW(I&S)

before industry data collection with minor clarification of terms but otherwise no substantive modifications. The focus areas were:

1. **Entity Clearance Eligibility and Access:** Preparing for and completing DOW's Entity Clearance Eligibility processes, commonly referred to as Facility Clearances (FCLs), including barriers-to-entry without Entity Clearances, delays in reviews and determinations, and Entity Clearance sponsorship opportunities.
2. **FOCI:** Preparing for and completing DOW's FOCI review process, including timelines for preparation and submission of materials, government risk assessment/review and determination process, mitigation action plans, and integration with other requirements.
3. **Safeguarding of Classified and Sensitive Information**:
    - Classified and Sensitive Information Risks: Identifying and safeguarding sensitive, controlled, and classified information consistently.
    - Classified Facilities: Navigating DOW's processes for accrediting facilities for classified work (e.g., secure facilities, Sensitive Compartmented Information Facilities (SCIFs), Special Access Program Facilities (SAPFs)), including interpretations of accreditation and audit requirements, approval authorities and delegation, and co-use and reciprocal use of facilities across departments/agencies.
    - Classified Systems and Networks: Navigating DOW's processes for accrediting and accessing classified networks and information systems, including fragmented policies across networks and programs, inconsistent implementation and interpretation of security requirements between policy frameworks and across departments/agencies, and updating policies for modern IT hardware and environments.
4. **Cybersecurity:** Securing classified and controlled information systems under overlapping government cyber policies, including conflicting, fragmented, and/or outdated security frameworks (CMMC, NISPOM, DFARS, and related guidance), and impacts to protecting data while adopting modern technologies such as cloud-native services, Software-as-a-Service (SaaS), Zero Trust, and automated monitoring.
5. **Integration of Security into Acquisition Processes and Contracts:** Identifying opportunities to require and incentivize security integration into solicitations and contracts by leveraging cross-functional collaboration, including acquisition security professionals, to develop work statements, evaluation factors, and performance measures that drive innovation, ensure secure systems, and build confidence in mission-critical technologies.

Though OUSW(I&S) approved the list, the FAST Study's data collection and analysis considered requirements, practices, and systems under the authority and responsibility of OUSW(I&S), DCSA, Defense Information Systems Agency (DISA), Defense Intelligence Agency (DIA), the DOW Chief Information Officer (CIO), NARA/ISOO, OUSW(A&S), and OUSW(R&E).

Subcontracting, small business, and NDC challenges were cross-cutting themes across the five focus areas rather than being additional focus areas. Data collection and analysis integrated the themes across all focus areas given the importance of enabling and expanding innovation in the DIB through easier, more scalable entry of small businesses and NDCs, and success in the defense market. Importantly, subcontracting was treated distinctly from small businesses and NDCs in line



with the SecWar's goal to negotiate and invest directly with all companies and suppliers throughout the DIB, not just through the big prime contractors.[1]

Some areas, while important, were deemed out-of-scope for the FAST Study due to being governed primarily outside the DOW (e.g., Intelligence Community Directive (ICD) 705 for SCIF construction standards) or significant reform efforts were already underway and over (e.g., personnel vetting under Trusted Workforce 2.0 (TW 2.0) overseen by the interagency Security, Suitability, and Credentialing Performance Accountability Council (PAC) PMO).[9] Other out-of-scope areas included classification and marking procedures, international security requirements such as export controls, certain personnel eligibility procedural details, non-cyber incident reporting, security training and briefings, visits and meetings, insider threat program specifics, and non-Department programs.

DATA COLLECTION PROCEDURE

Between July and November 2025, MITRE's behavioral sciences and security researchers designed and conducted semi-structured interviews to collect industry's detailed realities for timelines, decision points, implementation hurdles, impacts, and enablers for a range of government security requirements, practices, and systems. Figure 1 provides a list of topics used in the interview protocols, though specific topics were tailored to each company's expertise and experience with government security requirements and contracting. Appendix A provides a detailed list of interview topics.

1	**Most Challenging Security Requirements, Practices, and Systems**
2	**Entity Clearance Eligibility and Access, including DD Form 254**
3	**Foreign Ownership, Control, or Influence (FOCI)**
4	**Safeguarding Sensitive and Classified Information (e.g., CUI)**
5	**Security Classification Guides (SCGs), Program Protection Plans (PPPs), Technology Protection Plans (TPPs)**
6	**Classified Facilities (e.g., Collateral, SCIF, SAPF)**
7	**Classified Information Networks and Systems (e.g., SIPRNet, JWICS)**
8	**Cybersecurity and Information Security (e.g., CMMC)**
9	**Security Aspects of Subcontracting**
10	**Security Challenges in Business Development**

Figure 1. Consolidated Interview Topics for FAST Study

MITRE's behavioral scientists also designed and deployed online questionnaires for industry to share quantitative measures of burden and performance (e.g., days to Entity Clearance sponsorship decision; typical cost ranges for CMMC controls). Separate questionnaires were developed for facility clearances, FOCI, classified facility accreditation, information system authorizations,

[9] Security, Suitability, and Credentialing Performance Accountability Council (PAC) (2025). *Trusted Workforce 2.0 Quarterly Progress Review for January 2025*. Source: https://assets.performance.gov/files/FY25_Q1_Personnel_Vetting_QPR.pdf

cybersecurity, risk from people and information, and the security of subcontracting. Questionnaires included closed-format items and structured numeric inputs for cost, time, and workforce hours, accompanied by targeted open-ended prompts to capture context and emergent challenges. To reduce ambiguity and account for differences in maturity and capability, tailored questionnaire variants were developed for SMBs and NDCs. Each questionnaire took between 30 and 60 minutes to complete and most companies completed them in multiple sessions based on the need to retrieve relevant information.

In addition to interviews and questionnaires, MITRE's behavioral scientists conducted four additional focus groups to identify and prioritize options to manage challenges on specific areas. In those focus groups, business owners, security practitioners, and subject-matter-experts (SMEs) such as legal experts were invited to 90-minute sessions with 3 to 45 industry peers. Focus group topics included SMBs concerns, CMMC implementation, and National Defense Authorization Act (NDAA) 2020 Section 847 FOCI requirements.

For simplicity, all individuals who took part in the FAST Study are collectively referred to as *interviewees*, irrespective of the mode through which they contributed data.

ANALYSIS

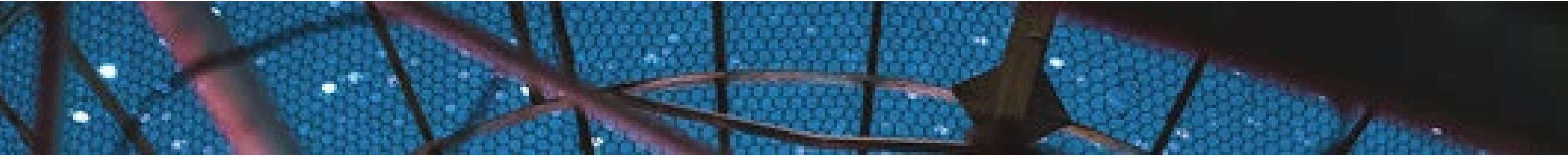
The FAST Study's team of MITRE behavioral sciences and security researchers, practitioners, and SMEs conducted systematic quantitative and qualitative analysis of industry data from interviews, questionnaires, and focus groups.

For qualitative analysis, the team used thematic analysis on interview and focus group transcription-like notes, in addition to open-text responses in the questionnaires. The team hand-annotated all of the qualitative data after developing a schema to align recurring challenges, impacts of those challenges, and recommended actions to mitigate those challenges. The team assessed thematic saturation within and across topics to ensure data coverage and to distinguish isolated anecdotes from persistent patterns.

For quantitative analysis, the team calculated descriptive statistics (e.g., frequency, means) based on numeric data in the questionnaires and thematic codes used during the qualitative analysis of interviews and focus groups. Through quantitative analysis, the team derived distributions for time, cost, and workforce hours associated with specific requirements and process steps, and (where possible) segmented results by industry type role and size. When quantitative data was incomplete, the team used conservative ranges grounded in multiple respondents and corroborated by qualitative evidence.

All challenges and recommended government actions were cross-referenced with publicly available laws, regulations, directives, manuals, and oversight materials by MITRE policy and contracts SMEs (e.g., Title 32 CFR Part 117, FAR, DFARS, DODD, etc.) to ensure alignment with current authorities and implementation practices.

To prioritize challenges and recommendations, the team applied a decision framework that considered: frequency and consistency of the challenge across respondents; materiality of burden

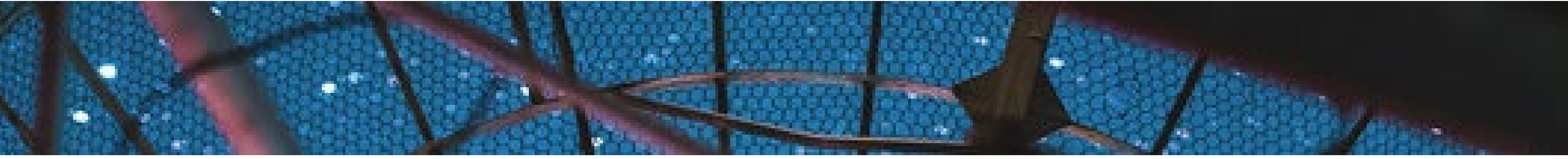


in cost, delivery time, and workforce hours; effects on equity and access for small businesses and NDCs; security risk if modified or streamlined; ownership; implementation feasibility; dependencies on external initiatives; potential for reciprocity and co-use; and opportunities for automation or technology support. Each potential challenge with recommendation was assigned an initial feasibility and impact rating. Recommendations with high burden reduction, clear ownership, low security risk, and near-term implementation were elevated.

For each prioritized item, the team synthesized the following information which is presented in the Analysis section for each focus area:

- **Challenge:** Specific acquisition security requirement, practice, or system that imposes material or undue impacts on cost, schedule, or performance.
- **Recommended Government Action:** Implementable action that clarifies, modifies, streamlines, automates, or cancels a requirement or practice, or pilots and evaluates a process change. Owner (e.g., OUSW(I&S), OUSW(A&S), DOW CIO), instrument (e.g., policy, DODI, implementation guidance), sequencing, and alternate implementation options are identified as relevant.
- **Impact for Warfighter:** Expected improvement to delivery speed, availability, quality, or mission risk reduction if the recommendation successfully manages the challenge.

Analysis underwent independent technical peer-review by MITRE industrial security researchers, practitioners, and SMEs in entity eligibility and FCLs, FOCI, classified facilities, information system authorizations, cybersecurity, insider risk/threat, and personnel vetting, as well as DOW policy and contracts SMEs. Peer-reviewers assessed analytic rigor, alignment with current authorities and implementation practices, feasibility and ownership, security risk and unintended consequences, and cross-domain consistency. Questions and comments were tracked in an adjudication log, resolved by the analysis lead with the relevant domain lead(s) and project leaders, and escalated for additional review as necessary.



3. FINDINGS AND RECOMMENDATIONS

The FAST Study's 74 challenges and 155 recommendations are organized by five focus areas: (1) Entity Eligibility and Access; (2) FOCI, (3) Safeguarding of Classified and Sensitive Information; 4) Cybersecurity, and (5) Integration of Security into Acquisition Processes and Contracts.[10]

ENTITY ELIGIBILITY AND ACCESS

Entity Eligibility is a key entry point for NDCs, small, and medium-sized businesses to begin work on DOW classified contracts. DCSA, acting as the Cognizant Security Agency (CSA) for DOW, makes an Entity Eligibility Determination as to whether a company is eligible for access to classified information of a certain level (e.g., Secret, Top Secret). Entity Eligibility Determinations are the gateway for companies to perform on classified contracts, requiring necessary (but not sufficient) conditions for access to classified solicitations, ability to submit employees for personnel clearances, use of classified facilities, and connection to classified networks. Delays or confusion in the Entity Eligibility process directly impact how quickly the DIB's innovative capabilities reach the warfighter. The process also strongly influences competition. This section will show the challenges for NDCs and small businesses trying to enter the market.

1) Lack of DCSA Problem-Solving and Connection to Warfighter Mission Reduces Security Enterprise Urgency

Challenge

DCSA has publicly and regularly branded itself as "America's Gatekeeper" in social media and its Strategic Plan (2025–2030) stating their mission as "secur[ing] the trustworthiness of the United States Government's workforce, the integrity of its cleared contractor support, and the uncompromised nature, services, and supply chains" (p.6).[11] There is an inherent disconnect that 80% of the FAST Study interviewees noted with DCSA's mission not being tied directly to the needs of the warfighter as determined by the MILDEPs. DIB contractors are required to work with speed and efficiency to get their innovative solutions to the warfighter. DCSA's "gatekeeping" is often experienced as an "in or out" mechanism rather than a "how can we assist you in supporting the warfighter mission with speed and efficiency."

> *"DCSA is an island unto itself, it is not tied to or tethered to any of the user agencies that are acquiring. They sit as a third-party arbiter."* – Industry interviewee
>
> *"[Even if you are trying to get] explicit capability in the hands of the warfighter [it requires] a lot of brute force because of disconnects."* – Industry interviewee

[10] Focus areas defined in *Section 2. Methodology.*

[11] DCSA (2025). *Defense Counterintelligence and Security Agency Strategic Plan 2025-2030.* Source: https://www.dcsa.mil/Portals/128/Documents/about/err/DCSA%202025-2030%20Strategic%20Plan%20Rev%201.pdf

> *"The fundamental flaw in our ecosystem is the disconnect between DCSA and the acquisition community—they're not tied together. There doesn't seem to be any linkage. It makes it very difficult to try to get anything done. When you compare and contrast with SAP, it is all about the mission – we are trying to put exquisite capabilities in the arms of the warfighter."* – Industry interviewee
>
> *"Where is DCSA's involvement left of launch? User communities are heading down the pathway to acquire a new technology—where is DCSA in that process? We need someone from DCSA or I&S to turn to being a service partner – we need you to provide this support!"* – Industry interviewee

Interviewees described disconnects between the support they need to provide innovative solutions at speed for the DOW and the "checklist mentality" of DCSA that is experienced as risk-averse and a hinderance to the NISPOM process. The DIB is requesting that DCSA be a service provider rather than a "gatekeeper", to better assist them in supporting the warfighter mission with speed and efficiency. Many interviewees reported that DCSA field representatives had a lack of understanding of the technologies being developed and then made security recommendations not in line with feasible outcomes. For example, one space contractor was directed to build two separate launchpads, one for commercial and one for government payloads, to mitigate perceived mission prioritization (commercial over DOW). The DIB company's response was *"we're never building two identical pads to launch the same rocket. That's not how space works."* This demonstrates a limited understanding of space industry operations and scheduling and drives unnecessary costs.

> *"Having DCSA more read into the technologies and make them more cognizant of the technologies that they are protecting or holding us to protecting."* – Industry interviewee
>
> *"…instilling in DCSA that a contractor can meet intent without it being a check box exercise. If representatives at DCSA were more in tune with what the contractor's business is they would better understand intents were already being met. How can they understand risk to national security if they don't understand what the contractor does?"* – Industry interviewee

In the FAST Study, many industry interviewees perceived DCSA as adopting a "policy will not allow it" approach to the detriment of the mission. The impact is that some companies assume security complications mean they are actually being denied entity eligibility, leaving companies paused and delayed in identifying what next steps to take within DOW complexity. For example, one industry interviewee described, "*it is like going to the DMV to update a registration, get a license, and a REAL ID; you have to go to three different windows and talk to three different representatives and none of them talk to each other.*" Another industry interviewee described: *"DCSA's serial, checklist culture contrasts sharply with IC's risk-based pragmatism."*

Several interviewees also reported that when they raised complex or cross-cutting issues, DCSA Industrial Security Representatives (ISRs) often signaled matters were outside their remit and directed companies to other groups, reinforcing the perception that no single DCSA touchpoint feels responsible for helping industry navigate end-to-end security challenges in support of the warfighter.

Recommended Government Action

The FAST Study recommends that DCSA shift its mission mantra from a gatekeeping culture to a warfighter service provider culture, prioritizing connections with the DOW acquisition and mission community allowing for more comprehensive support of the DIB supporting the warfighter mission. Figure 2 depicts the critical role that DCSA can adopt by shifting to a service provider culture. The shift will require an assessment and management of risk in the operational environment and a realignment of processes to emphasize speed and efficiency in providing innovative technologies and services to the warfighter. DCSA needs to take its priorities from the mission owners, not taking direction from the squeakiest wheels. In addition, new technologies are being developed rapidly and keeping up with them can be difficult. MITRE recommends that DCSA have access to government mission owners and SMEs in key technological areas (i.e., space) allowing for quick reach back with questions to avoid making security requests of DIB companies that are not feasible or that do not drive down risk. DCSA should not focus on developing its own cadre of SMEs, but instead developing strong relationships with the technological SMEs throughout the Department.

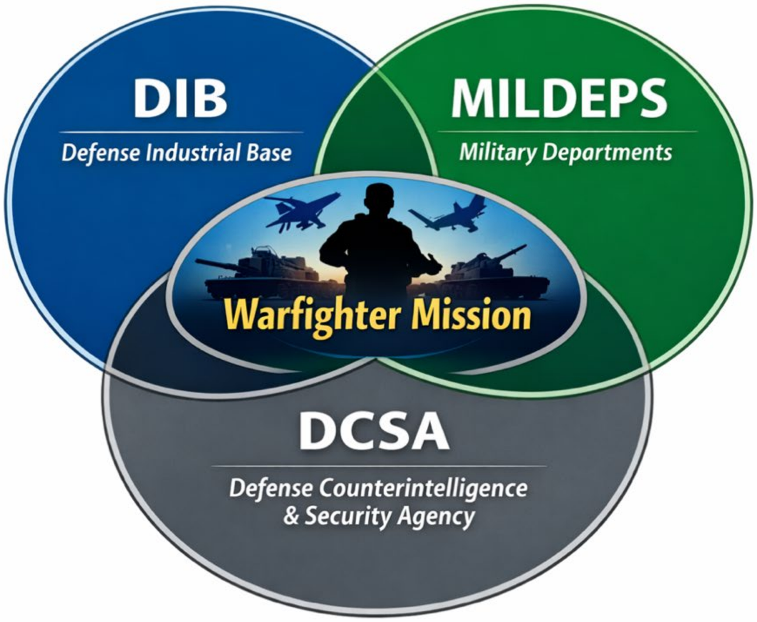
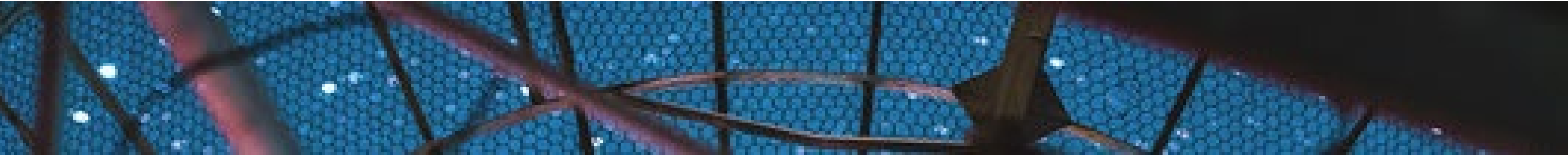


Figure 2. DCSA's Critical Role Supporting DIB and MILDEPs

In the short-term, DCSA should build upon existing relationships with DOW Military Departments (MILDEPS) to address ad hoc issues that arise. Furthermore, OUSW(I&S) should (1) direct DCSA to realign its central purpose and mission using a more risk-informed approach to safeguarding

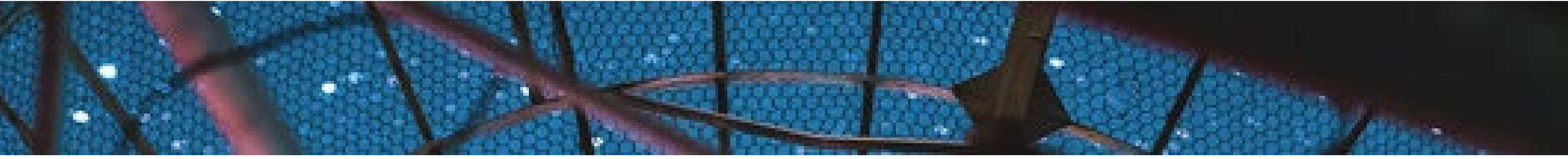


and supporting the warfighter mission, and (2) implement a formal group of representatives from the MILDEPs or the Defense Security Enterprise Advisory Group (DSEAG) tasked with engagement of tactical and operational components to help prioritize and adjudicate warfighter needs when backlogs occur. This office will form the connective tissue needed to represent MILDEP concerns and priorities to DCSA, quickly raising emergent DIB security processing or approval challenges at the speed of mission, thus adding a critical bridge between DOW, DCSA, and the DIB that has been notably missing in the process. DCSA should staff at least one dedicated, named liaison (e.g., "mission liaison") resident within DCSA and partnered directly with the above described formal group of mission operational representatives, serving as the primary, accountable POC for all DCSA–MILDEP interactions. This mission liaison would be responsible for real-time discussion of DIB challenges the mission deems critical for resolution. They would also routinely engage to identify and communicate back to DCSA the MILDEP's highest-priority security needs, ensuring those priorities inform decisions and backlogs, and resolving cross-cutting issues end-to-end to ensure timely expansion of the DIB.

> *"DCSA […] came a long way and have done good things. The question is how we continue to get them to be mission-oriented/focused and understand the importance of driving mission versus just black and white checklist thinking."* – Industry interviewee

Some DIB interviewees reported positive relationships with DCSA; however, many indicated that these relationships had to be cultivated over time to ensure appropriate access and responsiveness when needed. While such relationship-building can facilitate more effective partnering, it places new entrants to the DIB at a disadvantage, as they have not yet had the opportunity to establish comparable connections with DCSA personnel.

In addition, DCSA should adopt a more customer-service and problem-solving oriented mindset, shifting from a rigid "policy will not allow it" stance to a *security enabler* approach that focuses on "how do I enable this securely." DCSA needs to become an agency full of security enablers that focus on constructive problem-solving to proactively provide actionable guidance to industry and to connect industry to the appropriate resources to manage security risks. This mindset shift will require DCSA to cultivate intrinsic motivation and collaborative behaviors within its workforce. To provide mission-focused security solutions to their DIB customers, DCSA should also develop strong relationships with government mission owners and SMEs that will help ISRs understand, as necessary, emerging technologies. Industry interviewees described frustration trying to communicate risk mitigations with DCSA ISRs that did not have enough understanding of the work being performed or technologies being delivered. DCSA should adopt a facilitative role, convening the necessary government parties to collaboratively develop innovative security solutions that mitigate risk while advancing the warfighter mission. The changes would reposition DCSA as a proactive partner with the DIB in risk management, rather than being perceived as a gatekeeper slowing or preventing entry.



Impact for Warfighter

Connecting the mission full circle from requestor (DOW) to developer (DIB) to problem-solving, mission-focused service provider (DCSA) will bring a renewed focus on the broader warfighter mission, the need for speed and efficiency, how to best safeguard critical technologies, and reasons why safeguarding is so imperative. This renewed mission focus as a security support provider will expand the aperture for greater collaboration to meet overall mission needs while also supporting the distinct needs of each individual mission area. By maximizing efficiency through collaborative approaches and strengthening DCSA connections to the operational environment, DOW can increase speed while securely transforming warfighter capabilities. By adopting a security enabler mindset, DCSA can transition from being a gatekeeper to a trusted security partner with the DIB, helping them securely meet the DOW requirements.

2) DCSA Inconsistencies in Guidance and Decisions Delays Projects and Fosters DIB Frustration

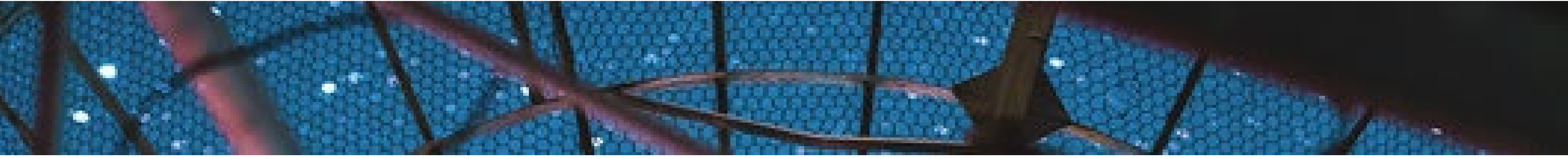
Challenge

DIB shared examples of ISRs and DCSA personnel providing valuable assistance and emphasized that many individuals within DCSA excel in their roles. While some DIB interviewees characterized interactions with DCSA as generally positive, many reported concerns in DCSA's guidance and decisions. Interviewees had concerns about the self-ascribed "DCSA as gatekeeper" model, in which ISRs view their role more as *enforcers* of rules than as *service providers* to DOW supporting DIB companies in securely and expeditiously delivering capabilities to the warfighter.

Interviewees also had concerns about inconsistencies spanning several key areas, including entity clearance determinations and cybersecurity-related matters. Interviewees noted variation in required processes and documentation, including DCSA requests for additional materials they perceived as unnecessary. They also cited differences in interpretations and expectations among ISRs, both within the same region and across different regional offices. Additionally, DIB interviewees reported inconsistent transparency regarding DCSA processes and timelines, including difficulty reaching program staff in a timely manner to address questions.

DCSA inconsistencies in guidance and decision-making have several negative effects. First, the inconsistencies increase cost and resource burdens for both DCSA and DIB companies, as companies undertake unnecessary additional steps. Second, the inconsistencies heighten frustration and confusion among companies, reducing their willingness to bid on DOW contracts. Third, these inconsistencies contribute to process delays that impede innovative DIB companies from rapidly delivering critical capabilities to the warfighter.

> *"Friction arises in compliance inspections due to inconsistent interpretation across DCSA field offices/regions. Same facts, different outcomes."* – Industry interviewee
>
> *"Everyone's aligned on the 'why.' We just need to make the plumbing faster and parallel, otherwise startups miss the window, and the mission slips with them."* – Industry interviewee

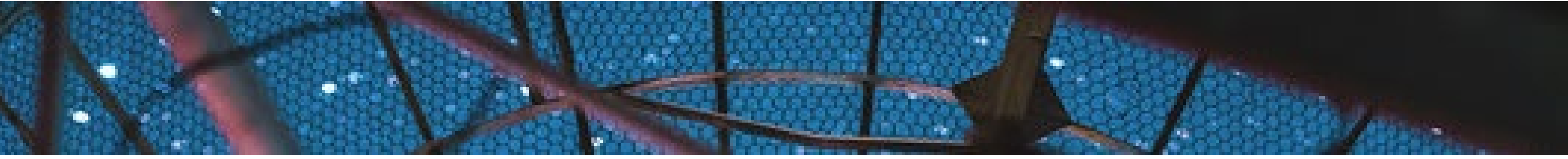


Many interviewees also characterized DCSA as frequently operating with a “checklist mentality,” which they reported contributes to delays, duplicative efforts, and confusion in its interactions with DIB partners. Interviewees expressed concern about DCSA’s reliance on this “checklist” approach, particularly in cases where the underlying risk it was intended to mitigate was not evident. The breadth of these concerns appears to stem from an organizational orientation within DCSA that emphasizes alignment of internal missions (e.g., personnel vetting, industrial security) and the gatekeeper role, rather than a risk-informed approach that prioritizes the secure and effective execution of the warfighter mission.

> *“DCSA’s serial, checklist culture contrasts sharply with IC’s risk-based pragmatism.”* – Industry interviewee
>
> *“…sponsorship package review seems inconsistent at VTU [DCSA Vetting Transformation Unit], with little deviation from a checklist mentality. Many times, all required items are accounted for within the SOW or draft DD-254, but the VTU reviewer is looking for a specific document or submission. The information is found within the SOW or PWS, but instead the package is rejected, and we have to go back to the customer for additional documentation.”* – Industry interviewee

Additional inconsistencies were identified under DCSA’s oversight, including with:

- Classified Cloud Approvals: Industry interviewees described inconsistency in how DCSA applies DFARS language to classified cloud, requiring contract-by-contract reviews of accredited cloud environments and invoking clauses that, in industry’s view, do not clearly apply to classified cloud, leading to different approval burdens for similar solutions.
- SIPR Provisioning and System Accreditation Sequencing: Industry interviewees stated that DCSA regions differ on when companies may submit system accreditation packages relative to facility inspections, with some regions insisting space must be fully approved first while others allow more parallel processing, resulting in different total timelines for establishing SIPR or onsite classified systems.
- Cyber Controls: Industry interviewees reported that certain cyber control families (e.g., encryption at rest and least privilege) and Cyber Operational Readiness Assessment (CORA)-related requirements are interpreted and weighted differently across DCSA reviewers, with some treating minor administrative issues as equivalent to critical vulnerabilities, producing inconsistent remediation expectations for similar findings.
- System Upgrade Approvals: Industry interviewees reported DCSA regional authorizing officials apply system change policies inconsistently. Some requiring full re-accreditation for routine actions such as operating system upgrades while others accept approaches like POA&Ms and scan evidence, resulting in different burdens for essentially the same change.
- Audit Documentation Expectations: Industry interviewees noted that some DCSA auditors required printed training certificates in physical binders for all cleared personnel, even when companies had invested in electronic learning management systems. Other auditors accepted digital records, resulting in different burdens for the same requirement.



Recommended Government Action

DCSA leadership should address the prevailing "checklist mentality" and update internal guidance and training materials to emphasize a risk-based approach. MITRE further recommends that DCSA institute a structured cross-regional calibration program. This could include periodic HQ-led case reviews, joint training across regions, and peer review of complex or precedent-setting decisions. The objective is to align interpretations and expectations among ISRs and regional offices, particularly risk-based application of NISPOM requirements and implementation.

To ensure better customer service to new entrants, DCSA should conduct a structured review of documentation requirements and process steps, with explicit consideration of risk versus burden. This review should identify anything that can be streamlined, consolidated, or eliminated without increasing risk, and should prioritize high-volume processes (e.g., routine audits, common system approvals) where duplicative or low-value requirements generate cost and delay.

Impact for Warfighter

Adopting a risk-informed, mission-focused security enabler approach to security processes will reduce unnecessary administrative and procedural burdens on both DCSA and the DIB. Streamlining processes and emphasizing efficiency will enable DCSA to focus resources on mitigating the most consequential security risks. By reducing process burdens for small businesses and NDCs, the DOW can expand the pool of capable industry partners, enhance innovation, and accelerate the fielding of new systems, tools, and technologies essential for maintaining operational advantage. Ultimately, these changes will strengthen the Department's ability to translate DIB capabilities into operational advantage, ensuring the warfighter is equipped to succeed in current and future operational environments.

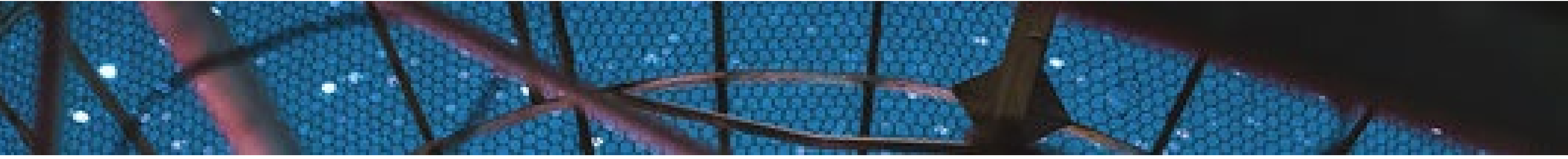
3) Facility Clearance Terminology Impedes DIB Entry

Challenge

Entity eligibility determination

An assessment by the CSA as to whether an entity is eligible for access to classified information of a certain level (and all lower levels). Entity eligibility determinations may be broad or limited to specific contracts, sponsoring agencies, or circumstances. A favorable entity eligibility determination results in eligibility to access classified information under the cognizance of the responsible CSA to the level approved. When the entity is accessing categories of information such as RD or SCI for which the CSA for that information has set additional requirements, CSAs must also assess whether the entity is eligible for access to that category of information. Some CSAs refer to their favorable entity eligibility determinations as FCLs. However, a favorable entity eligibility determination for the DHS CCIPP is not equivalent to an FCL and does not meet the requirements for FCL reciprocity. A favorable entity eligibility determination does not convey authority to store classified information. – *32 CFR 117.3*[12]

[12] Government Publishing Office (2025). 32 C.F.R. § 117.3 – *Definitions.* Source: https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-D/part-117/section-117.3



Entity Eligibility Determination requirements for access to classified information are provided in the National Industrial Security Program Operating Manual (NISPOM), or the 32 Code for Regulations (CFR), specifically in section 117.9. Paragraph 117.9(a)(5)[13] states that Entity Eligibility Determination can be referred to using the term *Facility Clearance* or *FCL*, and that term is used throughout the rule. However, *Facility Clearance* is often misunderstood, since area or facility accreditation of secure spaces is also a component of safeguarding classified information. As *facility* colloquially suggests physical space, new DIB organizations conflate *Facility Clearance* (an organization's eligibility to access classified information) with building and getting authorization for their spaces to store classified material; these are separate processes.[14] Alternatively, interviewees with Favorable Entity Eligibility determinations from other CSAs were not aware that *Facility Clearance* is an equivalent term and, therefore, treated the process as separate from the other CSA's Entity Eligibility Determination process. This confusion costs the DIB time and resources.

In discussions with government leaders, the FAST Study team learned alternative terminology was considered during earlier NISPOM revisions. However, only the DOW resisted *Entity Clearance* and preferred *Facility Clearance.* The compromise adopted *Entity Eligibility Determination* in the NISPOM, while explicitly recognizing *Facility Clearance* as an acceptable alternative or synonym.

Company Experience: A company with a Favorable Entity Eligibility Determination from a IC organization reported they pursued work with a MILDEP. When asked by the MILDEP for their FCL, the company did not know the term or that it was equivalent to their Favorable Entity Eligibility with the IC organization and went through the entire DOW Entity Eligibility process unnecessarily.

Recommended Government Action

Given the SecWar's goal of bringing innovation and new technologies of small, medium, and NDC companies into the DIB, the government should prioritize clear, consistent acquisition security language and requirements. To clarify the intent of Entity Eligibility Determination,[15] OUSW(I&S) should issue near-term implementation guidance (e.g., DOW Memorandum) to deprecate the term *Facility Clearance* or *FCL* and replace it with *Entity Clearance.* Consistent with personnel clearance terminology recommendations,[16] *Entity Clearance* should also be paired with *Eligibility* and/or *Access* to denote a company's current involvement in classified work. As with PCLs, access is determined by government contract. While deprecating *Facility Clearance* will require updates to legacy systems and established policy, NISPOM has used the term *Entity Eligibility Determination* for more than 20 years. Aligning nomenclature government-wide

[13] Government Publishing Office (2025). *32 C.F.R. § 117.3 – Definitions.* Source: https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-D/part-117/section-117.3

[14] The Entity Eligibility Determination section (§ 117.9(a)(3)) specifically states that "determination for entity eligibility is separate from determination of classified information safeguarding capability."

[15] Government Publishing Office (2025). *32 C.F.R. § 117.9 – Reporting requirements*. Source: https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-D/part-117/section-117.9

[16] See *Terminology Ambiguity in Personnel Clearances (PCL)*

improves clarity for NDCs, small- and medium-sized businesses by associating clearance with the company rather than a physical location for classified work and will enhance reciprocity across CSAs.

During the next 32 CFR 117[17] revision, the term *Facility Clearance (FCL)* should be removed from all sections in the rule, and other applicable documents, and replaced with *Entity Clearance (ECL)*. A note in the revised rule should alert users to the change in terminology but should reiterate that the term *Entity Clearance* is used for clarity and to differentiate the process from *Area and Facility Accreditation*. Table 2 provides an overview of the changes, including example definitions to describe the distinctions between Eligibility and Access. A company can have both eligibility and access, but not access without eligibility. For example, a company can have eligibility regardless of whether they have classified project work.

Table 2. Entity Clearance Terminology and Acronyms

Current Terminology	Proposed Terminology
Facility Clearance (FCL) or Entity Eligibility Determination	**Entity Clearance Eligibility (ECL-E)** Entity has been investigated and favorably adjudicated to a specific clearance level, suggesting the company (entity) can safeguard national security information to that level of clearance.
	Entity Clearance Access (ECL-A) Entity has been read-on and is currently working on classified projects. This status equates to having current access to classified materials.

Impact for Warfighter

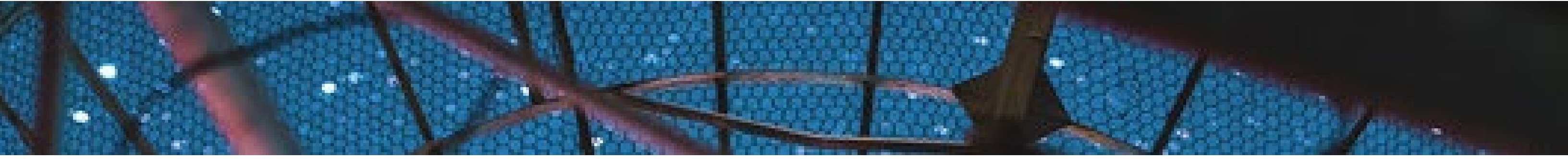
Words matter, and this one small change will dramatically support expanding the DIB. Clarifying *Entity Clearance* terminology will improve NDC's understanding of the government processes they must navigate to perform work on DOW classified contracts. It will also help reduce the misconception that companies must pay to build classified facilities which can be a deterrent for new entrants. By making terms clearer and more intuitive, government will reduce confusion, lower perceived barriers to entry, and enable more NDCs to pursue classified opportunities. Expanding the pool of companies able to propose competitive and innovative solutions will result in delivery of more advanced capabilities to the warfighter, enhancing battlefield advantage over adversaries who lack these solutions.

4) Lack of Entity Clearance Eligibility Sponsorships Creates Barriers to Entry

Challenge

Companies seeking to enter classified acquisitions with the federal government, specifically DOW, must be "trusted" to access (and in some cases store and maintain) the classified materials and

[17] Government Publishing Office (2025). *32 C.F.R. Part 117 – National Industrial Security Program Operating Manual (NISPOM)*. Source: https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-D/part-117/?toc=1



information associated with these contracts. To do this, companies must be favorably evaluated for Entity Clearance Eligibility. The requirements for this process are outlined in 32 CFR 117.9. Companies pursuing Entity Clearance Eligibility are required by this section to be *sponsored for an Entity Eligibility Determination* (§ 117.9(a)(10) and have a *Need to Access Classified Information* (§ 117.9(c)(1)). NDCs, small companies, and medium companies attempting to pursue and perform classified work face three key challenges in this process:

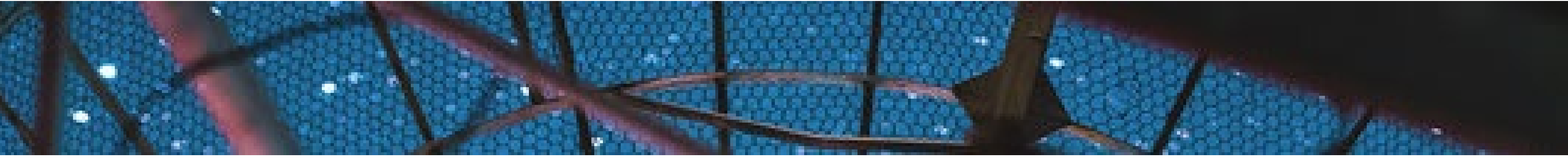
1. Government Contracting Agencies (GCAs) have not been willing (or lack understanding of how) to sponsor companies for Entity Clearance Eligibility (previously FCL). In the CFR requirement for companies to be sponsored for access, the rule states that either "a GCA or cleared contractor may sponsor an entity for an entity eligibility determination at any point during the contracting or agreement lifecycle."[18] Six interviewees suggested that GCAs and their contracting staff are not prepared to or aware of how to sponsor entities for an Entity Clearance. Reasons included that government contracting officers (KOs) or delegates are too busy to sponsor companies, have no experience or training in how to sponsor companies for Entity Clearances, or prefer that prime contractors handle the process. While these stated reasons have for the most part successfully absolved KOs and program managers of sponsorship responsibility, they dramatically constrain the entrance of small, medium, and nontraditional innovators into the DIB and over empower current cleared contractors, such as the big DIB companies, to determine which of these smaller companies get access to the Entity Clearances and consequently the DOW-cleared contracting environment. Additionally, SecWar in his statement on 6 December 2025, called out moving away from a prime contractor-dominated DIB to a "future powered by [a] dynamic vendor space that accelerates production by combining investment at a commercial pace."[19] To advance the Secretary's vision, GCAs must commit to actively sponsoring significantly more NDCs, small companies, and medium-sized companies for Entity Clearance Eligibility.
2. The Department of Defense Form 254 (Contract Security Classification Specification; DD-254) is the evidence most often used to substantiate an entity's "need to access classified information" for DOW classified solicitations and project work. In general, the DD-254 outlines the information and materials that must be safeguarded, what contractors will be allowed access to, the types of safeguarding measures that must be taken, and additional security requirements. Although government can create and disseminate the DD-254 <u>anytime during pre-award</u> (i.e., solicitation),[20,21] according to interviewees from all sizes of companies, the government rarely provides the form before contract award. This limits the ability of NDCs, small companies, and medium companies who are not yet in the DIB (i.e., new entrants) to be sponsored to and apply for Entity Clearance Eligibility.
3. Entity Clearance Eligibility through cleared contractor sponsorship is an alternative pathway for NDCs to initiate the Entity Clearance Eligibility determination to compete for

[18] Government Publishing Office (2025). 32 CFR § 117.9 – *Reporting requirements.* Source: https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-D/part-117/section-117.9

[19] Hegseth, P. (2025, December 6). *Remarks at the Reagan National Defense Forum* [Speech transcript]. Ronald Reagan Presidential Library, Simi Valley, CA. Source: https://www.globalsecurity.org/military/library/news/2025/12/mil-251206-dod01.htm

[20] 32 CFR §117.9 https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-D/part-117/section-117.9

[21] DOD (2006). *National Industrial Security Program Operating Manual (DOD 5220.22-M).* Section 6, Contract Security Classification Specification. Source: https://www.dau.edu/sites/default/files/Migrated/CopDocuments/DOD%205220.22%20M%20NISPOM%2020060228.pdf



DOW classified acquisitions. Interviewees suggested the prime-to-subcontractor process is more efficient than government sponsorship, as industry has a better understanding of the process. Additionally, these primes can provide mentoring and support on developing and managing security posture for NDCs looking to obtain an Entity Clearance. However, interviews with smaller companies suggested that (a) prime contractors were incentivized to subcontract with companies that already had an Entity Clearance Eligibility, (b) companies that entered into a subcontracting relationship accepted a reduction in financial margin, and (c) the process gives prime contractors significant power in the prime-to-subcontractor relationship which can allow the prime companies to have access to proprietary information and intellectual property from the sponsored company.

> *"The big issue is if government has to sponsor [an ECL], they don't understand DCSA like industry does which delays results. The government counterpart may be doing sponsorship for the first time. People rotate through jobs and there is not any legacy knowledge of the business process."* – Industry interviewee

Recommended Government Action

To expand the pool of companies with new and innovative technologies in the acquisition process, companies need to develop and disseminate DD-254 documents earlier in the acquisitions process. OUSW(I&S) and OUSW(A&S) should issue clarification guidance (e.g., DOW Memorandum) and formalize through a DODI that the preparation of the DD-254 for all classified contract acquisitions be completed[22] no later than solicitation (e.g., RFP) release. Having the DD-254 prepared at the solicitation stage enables government and prime contractors to sponsor small, medium, and nontraditional companies not yet cleared by the Entity Clearance determination process. Part of this guidance should include clarifying instructions to DCSA that Entity Clearance sponsorship with solicitation-phase DD-254s (i.e., pre-award stage) be processed in accordance with standard processing timelines and not delayed or assigned lower priority due solely to their pre-award status.

The Department should increase sponsorship of Entity Clearances for NDCs, small companies, and medium companies, strategically focusing on sponsoring companies capable of independently responding to solicitations for classified work and who have invested in their security infrastructure. OUSW(A&S) in partnership with OUSW(I&S) should issue clarifying guidance (e.g., DOW Memorandum) instructing GCAs to expand and responsibly exercise direct sponsorship of NDCs, small companies, and medium companies through the Entity Clearance Eligibility process. This approach aligns with the SecWar's call for direct government engagement with innovative companies and NDCs to expand the DIB.[23] The approach also aligned to FAST Study questionnaire data indicating 60% of responding academic institutions and 30% of SMBs describing their preference for government to be primary or sole sponsor for Entity Clearance, rather than prime contractors; this preference was also shared by six councils and consortiums or

[22] Without tailoring with company information.
[23] Hegseth, P. (2025, November 7). *Arsenal of Freedom* [Speech transcript]. National War College, Fort McNair, Washington, DC. U.S. DOW. Source: https://www.war.gov/News/Speeches/Speech/Article/4359074/remarks-by-secretary-of-war-pete-hegseth-on-the-arsenal-of-freedom-as-delivered/

Security-as-a-Service providers. KOs should provide the form included with Center for Development of Security Excellence's (CDSE) Facility Clearance (FCL) Sponsorship Instructions[24] (or a similar form) with all classified solicitations (e.g., Request For Proposal (RFPs)). This standardized form allows companies without Entity Clearance Eligibility to submit their information so that government acquisitions personnel can submit sponsorship information to DCSA in National Industrial Security System.[25] The guidance will also direct government acquisitions personnel (i.e., KOs, PMs, or acquisition security professionals) to submit Entity Clearance Eligibility sponsorship within a short period (e.g., 10 business days) following receipt of the information. In interviews, eight individual companies and six councils and consortiums or Security-as-a-Service providers described that government should release DD-254s with solicitations.

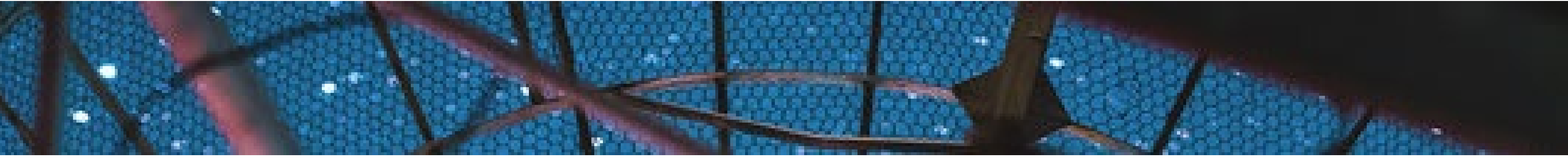
Prime contractor sponsorship of NDCs is a critical alternative to government sponsorship in the Entity Clearance eligibility process. OUSW(I&S) should further study the concerns NDCs, smaller companies, and some government interviewees had regarding this avenue of sponsorship. In particular, the proposed study should assess required or customary information sharing (e.g., SF-328 information, intellectual property), the degree of control over access to government sponsors, and the overall impact of sponsorship on financial margins to determine the need for additional guidance to sponsoring primes. Furthermore, the proposed study should explore options for incentivizing prime contractors to mentor and assist NDCs in strengthening their security posture and investments as well as sponsoring them for Entity Clearance eligibility.

Impact for Warfighter

This multipronged recommendation will significantly increase competition through DOW's engagement with and inclusion of NDCs, small companies, and medium companies within the acquisition process. The emphasis of this recommendation is for government to be more proactive in identifying and providing security requirements to all companies pursuing classified contracts. Additionally, these initiatives should encourage increased willingness from GCAs to sponsor NDCs and smaller companies in alignment with SecWar's vision for more direct commercial engagement. They also help manage risk by limiting government sponsorship of the Entity Clearance process to companies able to fully prepare and propose a solution to classified contracts while identifying feasible incentives for prime contractors to appropriately sponsor NDCs in good faith. Overall, these recommendations will expand the DIB to smaller and innovative companies through government sponsorship while continuing to support the current prime contractor to subcontractor process already in practice. Warfighters benefit from more competition and innovation delivered by an expanded pool of DIB companies able to start work upon contract award.

[24] Defense Security Service (2015). *Facility Clearance (FCL) Sponsorship Instructions*. Source: https://www.cdse.edu/Portals/124/Documents/jobaids/industrial/fcl-sponsorship-request-letter.pdf?ver=pD3CLNpLjYZtA13JBKLW7Q%3D%3D

[25] This process would be a manual copy from the CDSE form to NISS sponsorship data entry.



5) Complexity in Preparation of DD Form 254 Hinders DIB Expansion

Challenge

DD-254 is the primary form to justify a company’s need for classified access on government work and to sponsor an Entity Clearance Determination. Many interviewees claimed the government rarely provided the DD-254 during the solicitation phase and was often delayed providing it even after contract award. Not including the DD-254 during the solicitation phase adversely affects all prospective offerors, by preventing them from appropriately structuring proposals and allocating personnel and resources in accordance with security requirements. Furthermore, because the DD-254 is the primary justification for access to classified information, its absence at the solicitation stage precludes NDCs and small businesses from being sponsored by the government or a cleared contractor into the Entity Clearance process and limiting their ability to promptly start work upon contract award. These issues and the impact of cost overruns and project delays when DD-254 is delayed until after contract award make it imperative government employees prepare and disseminate DD-254s during the solicitation stage of acquisitions (see *Lack of Automation and Tools Hinders Faster Entity Clearance Package Reviews* for additional information). Nine interviewees suggested that a key reason for the absence or delay in the dissemination of DD-254 is government employees’ lack of understanding of the process for transcribing Critical Program Information (CPI) and required security safeguards into the DD-254. While training is already available from CDSE on preparing the DD-254,[26] some interviewees described their perception that government staff were not confident completing the form.

> *“They just didn't seem to understand the process. Really all they had to do was write a DD-254 that allowed us to have cleared subcontractors. We wrote it for them, and in the end even [when] doing that, it was ‘I don't know how’. Many iterations. Four to six iterations [over] weeks or months. They send us one, we mark it up with everything that was wrong with it.”*
> – Industry interviewee

Recommended Government Action

OUSW(I&S) in partnership with OUSW(R&E) and OUSW(A&S) should develop a user-friendly DD-254 Preparation Facilitator (PF254). This application should be a plainly written software application enabling government employees to prepare and revise a project’s DD-254 from solicitation through final project close. The PF254 will streamline entry of CPI, solicitation and contract information, and selection of safeguarding activities and requirements. The application should provide detailed instructions, FAQs, automated validation and error checking, and AI-driven recommendations to improve preparation efficiency. Additionally, the PF254 should include robust version control to track and manage DD-254 iterations at solicitation, contract award, in-contract revisions, and final closeout.

The current version of the DD-254 has an expiration date of 31 August 2028. Consequently, in the medium-term, the DOW and other CSAs should initiate a requirements-driven and feedback-

[26] CDSE (n.d.). *Preparing the DD Form 254 ISI28.16*. Source: https://www.cdse.edu/Training/eLearning/IS128/

driven overhaul of the DD-254. The overhaul should focus on reducing complexity for government personnel preparing the form so the DIB can receive clear, timely, and actionable security requirements. The DD-254 overhaul should be based on an analysis of the specific information DIB companies need to plan for in order to execute safeguarding of classified information.

The redesign should explicitly align DD-254 content and timing with early Program Protection Baseline activities and identification of CPI, CTI, and CUI to ensure that security requirements are both actionable for industry and synchronized with the acquisition lifecycle.[27] On behalf of the DOW, OUSW(I&S) could lead the effort with required coordination and concurrence from DOW CIO, OUSW(A&S), and OUSW(R&E), and input from DCSA and DOW Defense Office of Small Business Programs (OSBP) amongst others.

Impact for Warfighter

Deploying an intuitive, automated application to support government acquisition personnel in confidently and accurately preparing DD-254s will enable earlier, more consistent generation and dissemination of security requirements in the acquisition lifecycle. Accelerating DD-254 preparation will reduce project start delays, mitigate unanticipated security costs for industry, and provide timely justifications for NDCs and small businesses to initiate their Entity Clearance eligibility process sooner, rapidly expanding the pool of innovative companies and new technologies available to warfighters. Ultimately, equipping government employees with greater ability to document security requirements earlier and more accurately will strengthen and streamline the safeguarding of CPI across the defense enterprise.

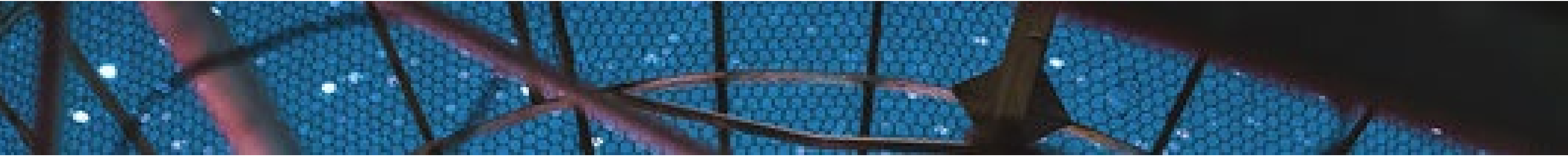
6) Lack of Automation and Tools Hinders Faster Entity Clearance Package Reviews

Challenge

Many interviewees described complexities and the manual, non-automated nature of preparing Entity Clearance packages. Industry interviewees described the current process as reliant on email exchanges, manual review of materials for errors and missing information or documents, and piecemeal fix requests and responses. Government interviewees reported more than 50% of industry's initial submissions contain errors, or are missing information and/or documentation. Industry did not refute this claim. However, industry interviewees also reported that DCSA does not conduct a comprehensive initial triage/check on the entire Entity Clearance package. Instead, DCSA is perceived as identifying errors in a piecemeal manner; additional errors are identified only after industry corrects previous errors. Piecemeal processing results in multiple back-and-forth iterations and long delays during DCSA's triage of Entity Clearance packages.

In part, FAST Study findings demonstrate industry challenges with data management and attention to detail when preparing their submissions to DCSA. Equally, findings also demonstrate DCSA's

[27] See: *Programs Begin Without CPI, CTI, CUI and Fail to Establish Early, Authoritative Protection Plans* for more information on earlier government engagement to establish Program Protection Baseline



guidance and Entity Clearance instructions are not clear or precise enough for industry to consistently and accurately complete the package. Interviewees described the delays and the piecemeal identification of errors as frustrating and requiring constant attention to keep the process moving to not further delay an already long clearance process. This challenge primarily affects NDCs and small companies that are preparing their first Entity Clearance packages or have submitted only a few packages, rather than larger firms that routinely complete them for new sites or Commercial and Government Entity (CAGE) codes.

> *"[Recommend] expanding the Triage and Vetting organization within DCSA to provide more resources for near real-time support via virtual meetings to assist in the processing and reduce the number of potential errors, delaying the process."* – Industry interviewee

Recommended Government Action

DCSA should employ automation and innovative tools in the receipt and initial triage of Entity Clearance package submissions. Half (i.e., eight) of the 16 large companies completing questionnaires specifically described the need for automation, AI, or innovative tools to help improve the Entity Clearance process. The process would benefit from tools that can quickly review forms; automatically cross-check information across submitted documents, sponsor submissions, and on SAM.gov (e.g., for CAGE codes and associated company information); and highlight missing information and documents to generate a comprehensive triage report. DCSA staff could then review this report for accuracy before it is automatically returned to the company for revisions and resubmission.

DCSA also needs to embrace and support transition of innovative tools to assist companies in completing their Entity Clearance package. The large number of frustrated comments from industry and the high error rates discussed by government suggest the need for additional support for industry beyond the *Facility Clearance Orientation Handbook*.[28]

In industry interviews, six separate organizations including three consortiums and one Security-as-a-Service provider specifically described the need for improved automated error checking of Entity Clearance Eligibility package submissions. Defense Advanced Research Projects Agency (DARPA) has laid groundwork in developing innovative tools for Entity Clearance package creation with its SBIR contracts for Turbo Facility Clearance (TurboFCL)[29] prototypes (i.e., like TurboTax® but for Entity Clearance (FCL) paperwork). Under these TurboFCL contracts, two companies are developing user-friendly, easy-to-understand plain-English prototype solutions to help organizations identify, gather, and prepare required Entity Clearance documentation. These solutions feature easy-to-understand user questions, interfaces, templates, frequently asked questions, and automated error checking to reduce mistakes and missing information. Initial prototypes were scheduled for delivery in December 2025, with a pilot testing phase scheduled for 2026. DCSA should engage with DARPA to receive regular updates on the prototypes, lessons

[28] DCSA (2018). *Facility Clearance Orientation Handbook*. Source: https://www.dcsa.mil/Portals/91/Documents/CTP/Facility%20Clearance/FCL_Orientation_Handbook_10OCT18.pdf
[29] DARPA (n.d.). *Turbo Facility Clearance (TurboFCL).* Source: https://www.darpa.mil/research/programs/turbofcl

learned, benefits, and design-phase challenges; and to exchange recommendations, common errors, and other challenges observed with Entity Clearance submissions. DARPA should include these inputs in the testing phase of the SBIR contracts.

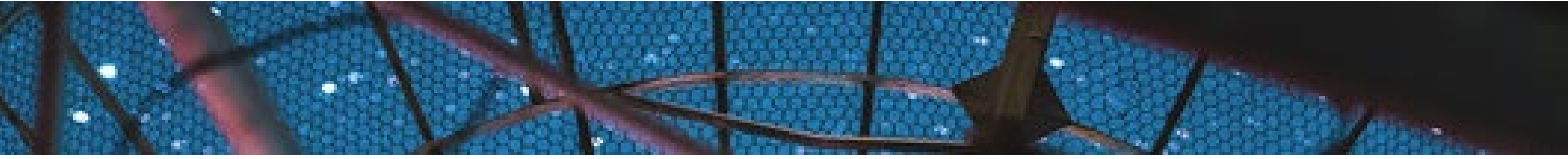
Upon completion of the DARPA TurboFCL pilot, DCSA should immediately partner with DARPA or conduct follow-on data collection and analysis to assess the impact of TurboFCL and comparable software on preparation of the Entity Clearance package versus manual methods. Key metrics should include: (a) time required for organizations to complete and submit the Entity Clearance package; (b) number and types of errors identified in the submissions; (c) volume and nature of organization activities requiring DCSA or other external assistance (e.g., lawyers, other cleared companies, consultants), and (d) systematic issues observed in TurboFCL-generated output provided to DCSA. Results should be analyzed and briefed to OUSW(I&S), OUSW(A&S), and the NISPPAC to identify the feasibility of TurboFCL and similar solutions as resources available to support organizations applying for an Entity Clearance. DCSA should quickly develop a standard Application Programming Interface (API), to ingest data from any TurboFCL-like solution into NISS (or its future replacement as part of the NISS Modernization, or NISS M, effort)[30] decreasing the need and cost of manual submission and exchange of packages.

> *"If there was development of DCSA phasing version of TurboFCL, it could have a dashboard with a queue showing where things [ECL package submissions] are in the process. This would help DCSA be faster rather than them receiving an email then having to download it onto their systems and move forward that way. It would increase speed and accuracy, reduce errors and the need for rework."* – Government interviewee

Impact for Warfighter

Automated solutions will save DIB and DCSA significant time and resources by decreasing the number of errors in Entity Clearance packages and by more wholistically and rapidly identifying issues that need to be mitigated before a human review of the submission. These solutions would reduce process complexity and lower the likelihood of delays caused by common errors in the Entity Clearance process. The solutions would also enable companies to quickly view their status in the process, reducing the number of emails sent to DCSA to check on status, and allowing DCSA staff to focus on other activities. In turn, automated tools enable the DIB to more quickly deliver classified, innovative solutions tailored to the warfighter's operational environment. Automated solutions support the President's Management Agenda[31] emphasis on leveraging technology and artificial intelligence to reduce processes and eliminate bureaucratic barriers.

[30] See *NISS Account Lockouts Cause Unnecessary Risk.*
[31] Executive Office of the President (2025). *President's Management Agenda*. Source: https://www.performance.gov/pma/



7) NISS Change Conditions Cause Holds, Creating Unnecessary Risk

Challenge

NISS, operated by DCSA, is the key system for “managing and overseeing industrial security of contractors working with classified information.”[32] DIB companies are required to use NISS to update their company’s information, referred to as a *change condition*, to maintain their Entity Clearance. This can include updates to Key Management Personnel (KMPs), company ownership, new sites, and FOCI, among other things.[33] Interviews with industry representatives indicated that change condition packages can take days to a year or more to receive approval. Six interviewees reported that each time a change condition package is submitted into NISS, the companies’ ability to submit *additional* change conditions is frozen (i.e., “locked-out”). The DIB can still log in and view information but cannot submit new change conditions or update the previously submitted package. Government officials explained that the personnel responsible for processing these packages are also tasked with conducting site visits and other operational activities, which are considered higher priority and frequently require them to be offsite (not in front of a computer). Although responsibility for change condition approval has since been centralized at DCSA Headquarters, delays persist due to competing priorities.

The “lock-out” was an intentional design decision and means that any reportable changes that occur after the submitted change condition package will require either 1) the company removes and updates the change condition package and basically starts the “lock out” and waiting process over again, or 2) holds all additional company changes until the current package is approved by DCSA and submits a new change condition package.[34,35] This process is inadvertently inserting risk due to the workarounds that some industry companies do to minimize how often their NISS accounts are frozen. Industry reports that the freezeout time can last from a few days to more than a year, regardless of type of reported change.

Many companies have approached this issue differently, which increases national security risk:

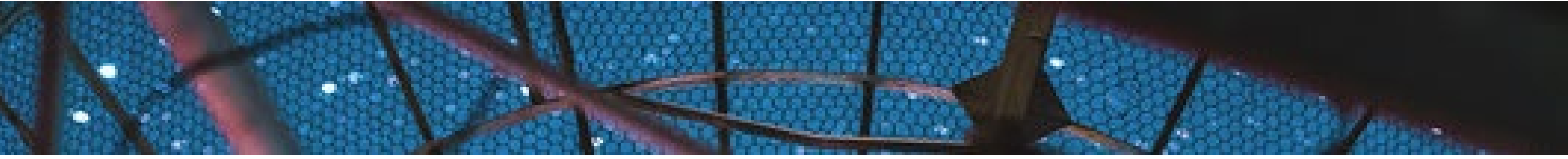
- Companies postpone submitting change conditions into NISS when anticipating further updates, so they can consolidate into one package.
- Companies noted that when they submit a change condition and later discuss an additional upcoming change with DCSA staff, they are directed to withdraw the initial package and resubmit a consolidated package containing both changes. This action effectively lowers their position in the review queue, extending the wait time before their case is processed and their ability to make additional changes in NISS is restored.

[32] DCSA (n.d.). *National Industrial Security System.* Source: https://www.dcsa.mil/Systems-Applications/National-Industrial-Security-System-NISS/

[33] DCSA (2021). *NISS 2.5 Release: Reporting Change Conditions*. Source: https://www.dcsa.mil/Portals/91/Documents/IS/NISS/DCSA_NISS_Factsheet_051221.pdf

[34] Defense Security Service (2019). *Reporting a Change Condition Industry User guide*. Source: https://www.cdse.edu/Portals/124/Documents/webinars/external-reporting-a-change-condition.pdf

[35] CDSE (2019). *Reporting a Change Condition Industry User Guide*. Source: https://www.cdse.edu/Portals/124/Documents/webinars/external-reporting-a-change-condition.pdf



- Some companies follow the process of submitting change conditions as requested, waiting for approval and the subsequent unlocking of their account before submitting the next change. This sequential approach results in delayed information sharing that risks overlooking additional changes or failing to report issues of potential concern in a timely manner.

> *"When there is need for resubmitting, everything has to be put back into the tool in order to submit it again. [I recommend to] rework this so the tool retains the originally submitted documentation as this eliminates rework and streamlines the resubmittal processes."* – Industry interviewee
>
> *"If they simply provided a PDF version of the change condition submission and allowed it to be modified with version control, that would seem like an easy fix. The way it currently locks us out creates headaches."* – Industry interviewee

DCSA is currently developing an update to the NISS, referred to as NISS Modernization or "NISS M", under the NI2 (NISS Increment 2) ongoing project to "incorporate current and emerging workflows and analytic functions required to support the Industrial Security mission to include the NISP Contract Classification System (NCCS)[36] bridge solution, Section 847 (Pilot) and NISS function into a cloud environment."[37] Government leaders stated that the current NISS has been put in sustainment until NI2 is released, which is anticipated in 18-24 months (approximately mid- to end-2027). Therefore, updates and changes to the NISS outside patches and fixes to maintain the system's current operation are limited. This means that the change condition submissions will continue to freeze industry out and lead to delays in updating government with additional corporate conditions until NI2 is developed and deployed.

The FAST Study team was informed that changes to NISS are in development at DCSA and will be *released earlier for other initiatives* (i.e., graphical tracker for Section 847 requirements) but *will not be incorporated* into the current NISS or be available for the current Entity Clearance Eligibility process until NI2 is fully released in 2027. Consequently, industry will have to rely on the existing system's shortcomings and experience significant delays and inefficiencies with NISS while waiting for NI2. The delays and inefficiencies create further downstream implications, such as delays in processing new Entity Clearances and potential loss of defense contractors due to current complexities and the time-consuming nature of the Entity Clearance process.

Recommended Government Action

While DCSA is currently working on NISS M, a modern system upgrade to NISS, the FAST Study proposes a short-term recommendation to reduce the unnecessary risk of the change condition

[36] DCSA (n.d.). *National Industrial Security Program (NISP) Contract Classification System (NCCS).* Source: https://www.dcsa.mil/Systems-Applications/National-Industrial-Security-Program-NISP-Contract-Classification-System-NCCS/

[37] DCSA (2024). *DCSA Industrial Security Program: Priorities, Issues & Answers*. Source: https://www.nsi.org/Impact24AttendeeDocs/IMPACT%2024%20DCSA%20Industrial%20Security.pdf

account freezes. Specifically, DCSA should improve the efficiency of reviewing and approving change conditions for Entity Clearances. The FAST Study recommends empowering DCSA senior regional staff, such as regional mission directors and field office chiefs, to support the review and approval of change conditions. Leveraging senior regional resources would distribute workload more effectively, improve timeliness, and reduce delays.

Current senior DOW priorities are to incorporate innovation through speed and efficiency in the acquisition process. To do this, DIB contractors, especially NDCs, need support to move through the Entity Clearance Eligibility process much faster than they can today. To accomplish this, NI2 must function as a truly modernized industrial security platform rather than a set of incremental adjustments layered onto legacy workflows. DCSA and DOW should treat NI2 as a fundamental modernization of NISS and not an incremental patch to align the system with some of the needs of the modern DIB. DCSA should re-prioritize implementation of the complete NI2 to 2026, given it is currently a significant bottleneck/impediment to DIB onboarding and managing DIB risk for classified DOW work. The NI2 effort and its capabilities should be rapidly accelerated and include versioning controls for change conditions, graphical status tracking, automated error and missing information checks on all forms, improved ticketing, API integration (e.g., TurboFCL), and other modern features. Accelerating NI2 is aligned with the President's Management Agenda[38] directive to consolidate and standardize Federal systems while eliminating duplicative legacy tools. Appendix B outlines Entity Clearance challenges and recommendations for solutions that should be prioritized for integration into NI2.

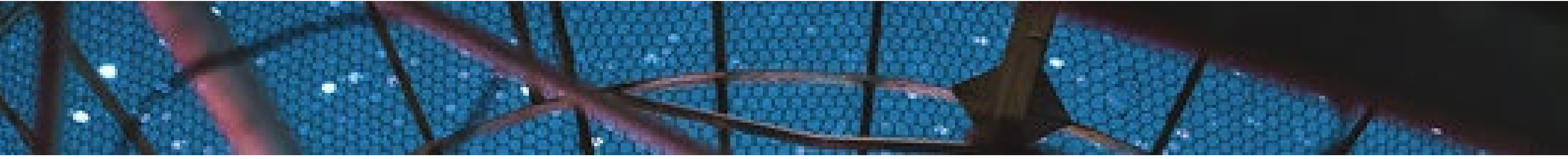
Consequently, DCSA will need to reprioritize other efforts to focus on completing the NI2 modernization. Current DCSA funding for other efforts should be reprioritized to expedite modernization of this critical system. Congress has already allocated significant funding to DCSA for NI2; therefore, the DOW security leadership, taxpayer, and DIB rightly expect return-on-investment at the speed of mission.

> *"NISS always presents a challenge, but that's more about system functionality than anything. Buttons don't always execute the tasks, fields don't always cooperate, etc.*"
> – Industry interviewee
>
> *"I would get it off the current platform. That platform [NISS] is old and outdated, it's difficult to log in, it's difficult to maneuver within. It's just not user friendly at all!"*
> – Industry interviewee

Impact for Warfighter

Significant delays processing Entity Clearance package submissions—when the process is paused due to DCSA approval of change conditions or while industry addresses requests—create real challenges and unreasonably extend timelines for industry applicants. These delays affect project starts and timely correction of deficiencies, heightens sponsor concerns, and increases process

[38] Executive Office of the President (2025). *President's Management Agenda*. Source: https://www.performance.gov/pma/



burden and frustration. Reducing delays in clearance change condition processing and increasing transparency will efficiently and effectively reduce barriers to entry and expand the pool of innovative and new technologies that can be more rapidly provided to the warfighter.

8) Outdated Facility Clearance Orientation Handbook Increases Subcontractor Confusion

Challenge

Interviews with DIB companies highlighted confusion about required documentation and where to locate guidance, making the Entity Clearance Determination process difficult to navigate. In January 2025, industry and DCSA held a two-day working group to streamline and clarify the DCSA *Facility Clearance Orientation Handbook.*[39] At least four members of councils and consortiums described how the working group's proposed feedback on the Handbook has yet to be implemented. The Handbook has reportedly not kept up with changes and requires additions to make it more comprehensive and centralized.

> *"FCL process is long and convoluted, especially for FOCI and new FOCI companies. We've been working with [DCSA] to try to help with a FCL handbook for industry. The way [the Handbook] reads now is difficult. [The] FCL process should be dummied down more."*
> – Industry interviewee

A 2023 report stated DCSA's *Facility Clearance Orientation Handbook* was fragmented across four websites and 18 guides, with critical details only accessible by downloading specific documents to open embedded attachments.[40] Materials provided by DCSA reportedly skew toward readers with security or government experience which risks alienating many NDCs and small businesses with limited DOW or government experience. The authors note that the Handbook emphasizes compliance references over step-by-step "how to" workflows, with limited examples, checklists, or timeline expectations.

> *"[Recommend] improving the training resources and FCL Handbook for FCL sponsorship and sponsored entity training, with detailed outlines of the requirements and required documentation, especially for smaller facilities or FSOs unfamiliar with the FCL sponsorship [process]."* – Industry interviewee

Recommended Government Action

DCSA must update and expand the *Facility Clearance Orientation Handbook*, recommended to be renamed as the *Entity Clearance Orientation Handbook*, and related documentation to simplify the process and improve transparency. To address dispersed resources and resulting industry

[39] DCSA (2018). *Facility Clearance Orientation Handbook*. Source: https://www.dcsa.mil/Portals/91/Documents/CTP/Facility%20Clearance/FCL_Orientation_Handbook_10OCT18.pdf
[40] Astafan, S.L, Browning, M.S., Bushong, B.W., & Rienstra, G.S. (2023). *Industrial Security as a Barrier to Non-traditional Vendor Participation* (Capstone Applied Research Project Report). Naval Postgraduate School. Source: https://calhoun.nps.edu/handle/10945/72487

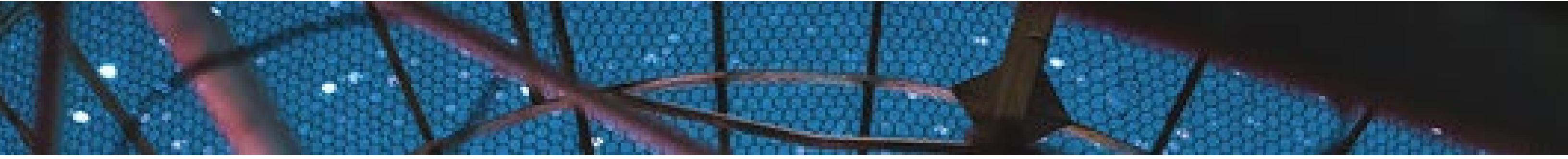
confusion, the FAST Study recommends that DCSA, under OUSW(I&S) oversight, update this information within six months of receiving the FAST Study report. This rapid action is consistent with the SecWar's request for rapid acquisition reform by actively mitigating uncertainty and reducing the resource burden associated with locating applicable content across multiple DCSA sources for the expanding DIB. Finalization of the Entity Clearance Orientation Handbook may require an additional joint working group session with DCSA and industry. The recommendations from industry span the full Entity Clearance lifecycle from before a company has an Entity Clearance through termination. Table 3 provides specific actions critical to providing the DIB with a comprehensive, up-to-date Orientation Handbook as requested during industry interviews.

Table 3. Industry Requests for Entity Clearance Orientation Handbook Updates

Industry Request	Government (DCSA) Key Actions
Recommend Pre-Entity Clearance Checklist	Develop a pre-Entity Clearance checklist that provides new entrants with prerequisites upfront, including PKI certification initiation for token requests, to reduce delays and extension requests
Provide industry with timelines for the Life Cycle of the Entity Clearance	Publish a Handbook section with expected timelines for the Entity Clearance Life Cycle, including submission requirements and concurrent actions
Sponsorship handbook for Sponsors completing DD-254	Develop and disseminate a Sponsorship Handbook that includes a comprehensive checklist for completing DD-254 to aid government and industry sponsors
Provide list of resources to contact for Entity Clearance submission advice	Compile a resource list with direct contact information to provide timely answers to Entity Clearance questions at all stages of the process
Provide FAQ section in Handbook	Create a FAQ section that addresses common challenges faced by industry in seeking Entity Clearances, offering concrete answers to the "what if" scenarios
Clarification on KMP subsection for PCLs	Clarify in a KMP subsection the distinction between essential and non-essential KMPs, with examples and descriptions of eligible personnel
Add post-Entity Clearance process to Handbook	Outline the steps following Entity Clearance award, including the initial orientation meeting with an ISR
Add Entity Clearance discontinuation section	Provide industry with detailed information on procedures when Entity Clearances are discontinued, including timelines for dormancy

Impact for Warfighter

Step-by-step guidance and standardized templates further accelerate capability delivery by minimizing submission errors and rework. Shorter clearance cycle times mean contracts can begin earlier, allowing innovative solutions to reach the warfighter faster. Plain-language, role-specific materials also expand DIB participation by helping small and nontraditional companies navigate clearance requirements. This broadens the industrial base, increases competition, and injects new ideas into the defense ecosystem, all of which strengthen operational effectiveness. Published workflows, timelines, and checklists give the DIB clear visibility into requirements, enabling them



to plan milestones and staffing more effectively. This reduces start-up delays and ensures programs are ready to deliver capabilities on schedule.

Streamlined onboarding to the Entity Clearance process also improves surge responsiveness. By enabling faster Entity Clearance Eligibility for new facilities, the DOW can quickly mobilize additional DIB support to meet urgent or emergent operational requirements. Lower costs from reduced rework and fewer delays further ensure that taxpayer resources are used more efficiently, allowing more funding to be directed toward mission-critical needs. For the DOW, it means a more agile, competitive, and secure industrial base that is better aligned with operational priorities and national security objectives.

9) DOD Enhanced Security Program Underutilization Reduces Innovative Problem-Solving

Challenge

The DOD's Enhanced Security Program (DODI 5205.85; DESP)[41] was developed and released for DOW to rapidly have classified conversations with industry SMEs or senior leaders who do not have clearances and are not employed by a company with an Entity Clearance. During FAST Study interviews, it became apparent that industry is both unaware of the DESP and deems it to have limited practical use. None of the industry companies interviewed were aware of the DESP.

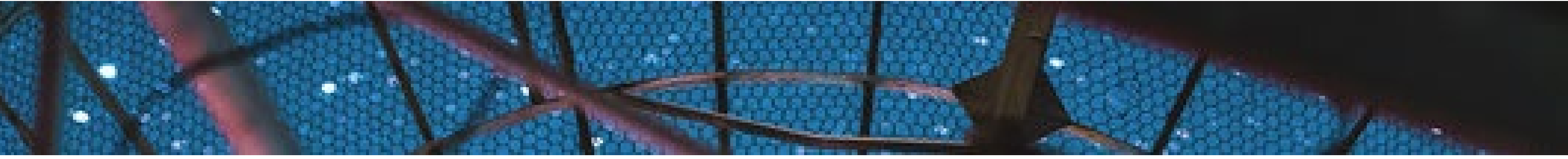
After being made aware of the program, industry interviewees described DESP as a great idea with little value because of its Secret level availability when most of the work it would support requires Top Secret level availability. Furthermore, industry also described that the use of DESP was limited if solely for conversations rather than to other practical uses. While the DESP does not limit its use to project work, there is no evidence it has been used for other innovative purposes (e.g., classified solicitation review) beyond its original purpose.

> *"We can't get our engineers in the room, and we can't get our BD [Business Development] team to hear the real problems. So, we're locked out of solving them."* – Industry interviewee

Recommended Government Action

OUSW(I&S) should extend DESP to Top Secret level information and announce the change broadly, including at the NISPPAC. The process for DESP-eligible company personnel to be granted Interim Top Secret clearance remains longer than desired (approximately 180 days). However, the ability of industry SMEs or senior leaders to engage in Top Secret classified conversations with cleared DIB and government agencies to prepare for submissions to classified acquisitions will likely expand its use by industry.

[41] OUSD(I&S) (2022). *DOD Instruction 5205.85: Enhanced Security Program to Support the DOD Innovation Initiative.* Source: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/520585p.PDF



OUSW(I&S) should provide clarification or guidance about the use of the DESP in DOW classified acquisitions. DESP excludes companies applying for or already possessing an Entity Clearance so as not to duplicate processes. However, the DOW is focused on increasing participation from NDCs in the DIB including in classified work. Many of those companies have difficulty being sponsored for an Entity Clearance because they are not seriously considered for classified work until they have an Entity Clearance. However, they cannot get an Entity Clearance without a "need to access classified information" which often occurs during award of a classified contract. To overcome the circular dependency between establishing need-to-access and obtaining sponsorship for Entity Clearance, OUSW(I&S) should issue implementation guidance (e.g., a DOW Memorandum) allowing companies to use the DESP for a small number of technical experts and business development staff to review and respond to classified solicitations ***prior to*** their company being sponsored for an Entity Clearance. Guidance should specify eligibility criteria, time limits, audit and custody controls, and immediate initiation of Entity Clearance sponsorship upon downselection.

Impact for Warfighter

Current SecWar priorities are "transform the entire acquisition system to rapidly accelerate the fielding of capabilities and focus on results."[42] He further emphasized moving to a "dynamic vendor space that accelerates production by combining investment at a commercial pace."[43] Expanding the DESP classification ceiling improves the value of conversations with temporary clearance holders, and prompts more innovative classified conversations. Extending its use by NDCs and small companies to review and respond to classified solicitations responsibly expands the vendor space. Ultimately, these changes appropriately expand DESP while maintaining the security required to safeguard classified information and deliver new technologies and innovation to the warfighter.

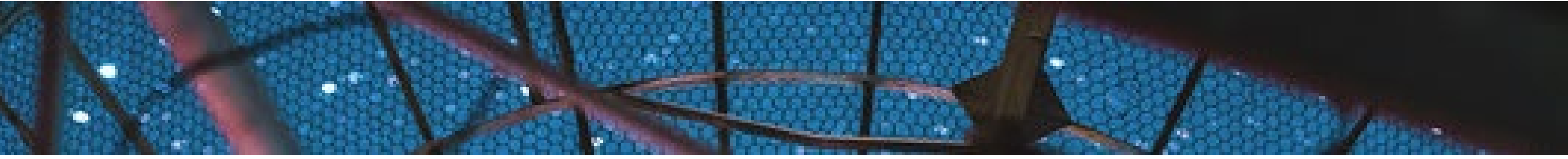
10) Lack of Co-Use Spaces for Classified Proposal Development Restricts Competition

Challenge

Smaller DIB companies and those without ability to access and store classified materials at their company (e.g., non-possessing Entity Clearance) often lack access to view and respond to classified RFPs and Requests for Information (RFIs), severely limiting competition and hindering innovation. Similarly, interviewees from these companies reported difficulties in obtaining entry to spaces required for responding to classified solicitations or often called "reading rooms" to access necessary RFP related documents/materials to inform their understanding of the RFP requirements and propose accordingly.

[42] Hegseth, P. (2025, November 7). *Remarks at the National War College [Speech]*. National War College, Washington, DC.

[43] Hegseth, P. (2025, December 6). *Remarks at the Reagan National Defense Forum [Speech]*. Ronald Reagan Presidential Library, Simi Valley, CA. Defense Visual Information Distribution Service. Source: https://www.dvidshub.net/video/989122/hegseth-speaks-reagan-national-defense-forum



These non-possessing cleared contractors may be eligible to view certain active classified RFPs and RFIs but must often have to gain approval to access cleared facilities to review the materials in the respective "reading room." This may require companies to travel to "reading rooms" located at geographically dispersed sites to access these materials and prepare proposals.[44] This process limits responses from new and innovative companies and increases company proposal costs, particularly for small companies. In addition, access to classified "reading rooms" requires strict need-to-know approvals, potential co-use agreements, and the ability to demonstrate mission relevance that can disproportionately affect newer entrants to the DIB.[45]

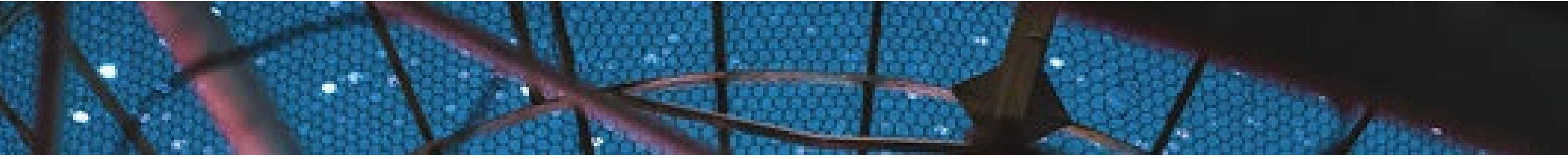
> *"Our organization has repeatedly encountered challenges in supporting and pursuing classified DOD programs due to the structural "chicken and egg" problem surrounding personnel and facility clearances. Although we design and manufacture technologies that directly support national defense missions (often through partnerships with prime contractors) we face barriers obtaining the clearances and facility accreditations necessary to compete independently for classified work."* – Industry interviewee
>
> *"Our lack of active classified contracts creates a circular problem: without a DD-254, we cannot clear key personnel or gain access to classified information needed to bid on or execute the work; yet without cleared personnel or systems, we are often excluded from the bidders list that would authorize the clearance/access needed. As a result, our teams are limited to unclassified participation in efforts where classified insight is essential for technical alignment and program planning. This has delayed our ability to respond to solicitations, limited our competitiveness in pursuing classified opportunities, and increased our dependency on prime contractors for access, despite having the technical expertise and required infrastructure to execute the work."* – Industry interviewee

Recommended Government Action

Interviewees proposed expanded access to classified "reading rooms" to view RFPs and RFIs as well as RFP-related documents/material to aid their proposal (or RFI response) development which should increase competition and innovation across the DIB. DOW should increase funding for and availability of government-hosted classified proposal reading and writing rooms. These rooms should be equipped with the Joint Worldwide Intelligence Communication System (JWICS) providing access to Top Secret Sensitive Compartmented Information (TS//SCI) and Secret Internet Protocol Network (SIPRNet) with print and scan capabilities. JWICS and SIPRNet terminals should allow access only to applications and segmented areas needed for proposal development, without unrestricted access, thereby preserving security.

[44] Classified reading rooms are tied to specific solicitations and contracting offices and require appropriate clearances. Contractor accessible reading rooms can be found at the Defense Information Systems Agency (DISA) Headquarters (Fort Meade, MD); specific Army Contracting Command (ACC) facilities; Air Force Life Cycle Management Center (AFLCMC) (Wright-Patterson AFB, OH); and regional Defense Contract Management Agency (DCMA) sites.

[45] Defense Technical Information Center (DTIC, n.d.). *DTIC Combatant Command (CCMD) Classified Reading Room*. Source: https://discover.dtic.mil/reading-room/



A standardized DOW-wide co-use template should be developed and adopted to streamline processes. Reciprocity across secure areas is essential for enhancing speed and efficiency within the DIB, enabling innovators to identify where their services and products are most needed. Secure sites should be approved as co-use spaces by default with exception waivers used in limited specific circumstances.[46] These co-use spaces should provide access to all classified DOW RFPs and RFIs in one platform when possible. RFPs and RFIs could be compartmentalized so DIB contractors are viewing requests specific to the products and service areas that they can provide. For example, compartmentalization of products and service areas could be done via Federal Supply Classes (FSCs)[47] which categorize products and services for government procurement, NAICS codes[48] which are used for industry categorization, or by DOW-specific mission area codes.[49] This may require integration of sites such as the System for Award Management site (SAM.gov)[50] and the DISA procurement site.[51] The physical environment where companies will conduct their proposal development should allow for both high side access to classified RFP/RFIs as well as temporary access to their company resources required during proposal writing.

> *"Can't bid without FCL; can't get FCL without award [leading to] reliance on prime sponsorship workarounds."* – Industry interviewee

DOW should consider Classified-Infrastructure-as-a-Service (CIaaS) providers as an option to enable more co-use spaces for classified proposal development. For example, to issue a DD-254 for an Entity Clearance, CIaaS providers could be required to provide a specific number of "reading rooms" and "writing rooms" and make them available to companies to view RFP and develop proposals. If the CIaaS model expands, the DOW should ensure protections are in place to avoid CIaaS providers effectively "picking winners" by allocating scarce classified space to the highest bidders. The Department should consider options that reduce pure profit incentives particularly for proposal development and contract execution. Facilities like these could speed access to "reading rooms" and "writing rooms." Executing this recommendation may require coordination with the appropriate officials at sponsoring agencies to determine what steps need to be taken to allow for co-use agreements specific to limited access classified reading and writing rooms. OUSW(I&S) should draft a memorandum stating that specific classified areas will be used for proposal development, that Defense agencies are expected to ensure these spaces are provided as co-use spaces, and that Defense agencies report back to OUSW(I&S) within 180 days to provide an update on the current status of government-hosted co-use reading rooms. OUSW(I&S) should coordinate with OUSW(A&S) on the reading room guidelines, access, and return-on-investment metrics.

[46] See: *Underuse of Co-Use Agreements Forces Redundancy and Underutilization*

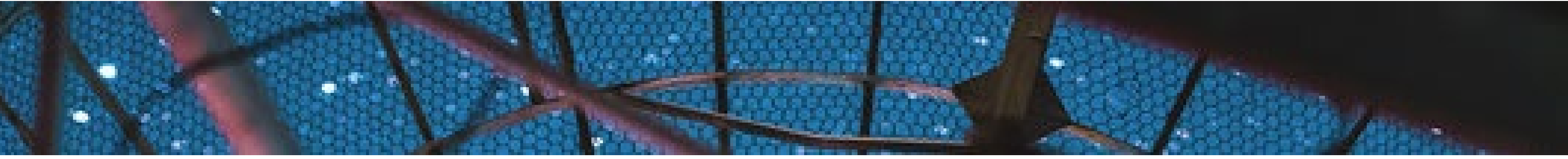
[47] Defense Logistics Agency (n.d.). *H2 Federal Supply Classification (FSC) Directory.* Defense Logistics Agency. Source: https://www.dla.mil/Working-With-DLA/Federal-and-International-Cataloging/H2/

[48] Census Bureau (n.d.). *North American Industry Classification System (NAICS).* Source: https://www.census.gov/naics/

[49] DOD (2006). *DOD Instruction 8115.02: Information Technology Portfolio Management Implementation.* Source: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/811502p.pdf

[50] GSA (n.d.). *System for Award Management (SAM.gov)*. Source: https://sam.gov

[51] DISA (n.d.). *DISA Procurement.* Source: https://disa.mil/About/Procurement



> *"Somebody says "no" [to reciprocity]. It's not their data though, it's the US Government's data and we're fighting a war against all bad guys. After [it is] established that the person has the right clearances and a need-to-know, then it's simply silly to not talk about it…then you've stifled innovation; it doesn't do anything to protect information."*
> – Industry interviewee

Impact for Warfighter

Barriers to entry, such as limited visibility of RFPs/RFIs and restricted competition in DOW classified contracts, impede timely support to the warfighter and can be rapidly removed. The use of co-use agreements and centrally located regional government-hosted co-use spaces is key to increasing speed and efficiency and allows the DIB to more expediently address the needs of the warfighter by reducing barriers to entry.[52]

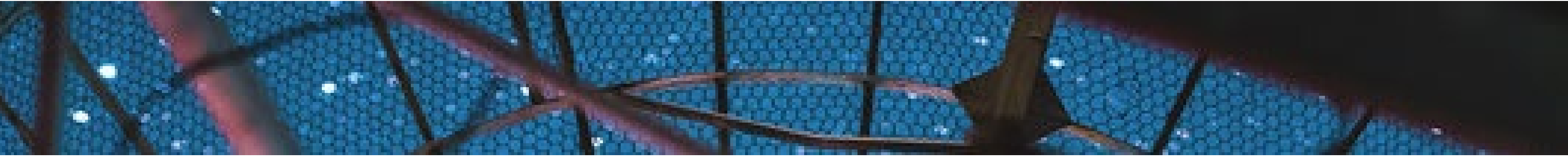
11) Cybersecurity is Not a Required Key Management Personnel Role, Leading to Systemic Technical Risk

Challenge

Rapid technology growth means the government and DIB must also rapidly integrate digital processes and technologies into operations to enable the warfighter. The USG and DIB are at daily risk from cyber threats with DIB reporting 64,399 actionable indicators of compromise related to safeguarding unclassified DOW information and intellectual property across networks.[53] As government acquisitions continue to design, develop, test, manufacture, and maintain innovation and new technologies for our warfighters in cyber and networked environments, it is essential companies working on classified contracts have a trained cybersecurity expert responsible for and prioritizing management and safeguarding of cyber environments.

Currently, the NISPOM does not recognize the critical role a cybersecurity professional plays in securing DIB companies working on classified contracts for the DOW as Key Management Personnel (KMPs). The 32 CFR 117.9 (Entity Eligibility Determination)[54] requires that companies submit a minimum of three KMPs to receive an Entity Clearance Eligibility. These roles are Senior Management Official (SMO), Facility Security Officer (FSO), and Insider Threat Program Senior Official (ITPSO). None of these roles are specifically expected to have cybersecurity expertise. The 32 CFR 117.7 (b) section on Contractor Security Officials, however, identifies the Information System Security Manager (ISSM) as a security official for those companies "who are, or will be,

[52] See *Underuse of Co-Use Agreements Forces Redundancy and Underutilization.*
[53] DOD Cyber Crime Center (DC3, 2024). *Department of Defense Cyber Crime Center Annual Report 2024*. Source: https://www.dc3.mil/Portals/100/Documents/DC3/About%20DC3/Annual_Report/DC3-Annual-Report-2024.pdf
[54] Government Publishing Office (2025). *32 C.F.R. § 117.9 – Reporting requirements.* Source: https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-D/part-117/section-117.9



processing classified information on an information system located at the contractor facility…" However, the role is not required to be a KMP.

> *"Give more importance to "I" [ISSM/ISSP] roles and not just when assessment fails or system needs to be shut down. It would help both government and programs to understand that it is a priority."* – Industry interviewee

Most large companies already have invested in cybersecurity professionals (e.g., ISSMs). However, NDCs and small companies face specific constraints in hiring cybersecurity personnel. In NDCs and small companies, employees trained in physical or facility security or another role are commonly asked to take on additional duties in managing the company's cybersecurity. In those circumstances, the company's cybersecurity could become the responsibility of leaders without the requisite cybersecurity experience or who deprioritize cybersecurity relative to their primary other duties (e.g., physical security).

Without a dedicated and experienced cybersecurity professional, NDCs and small companies risk compromise in an environment where threat activity is already high. The risk emerges from the companies being more likely to implement non-compliant ad hoc controls, misconfigure systems, and be unable to advocate and plan for key cyber investments. As FSO and ITPSO roles do not own cyber risk, cybersecurity is often deprioritized against physical security efforts, leading to stale patching, weak logging, delayed incident triage, and noncompliance with DFARS 252.204-7012[55] and CMMC[56] requirements. In addition to security risk, delivery risks are also increased. Companies without sufficient cybersecurity leadership experience delays to contract start dates, which drive cost and schedule risk for the company and the warfighter. The delays emerge from failure to close Plans of Action and Milestones (POA&Ms), failed or prolonged cybersecurity assessments, and delays to the Risk Management Framework (RMF) and Authorization to Operate (ATO). Poor cyber oversight of Managed Service Providers (MSPs) and cloud inheritance further produces inconsistent evidence, reciprocity failures, and avoidable rework. Ultimately, these shortfalls elevate cybersecurity and compliance risk, and slow secure delivery of capabilities to the warfighter.

> *"Industry needs to have highly skilled people who need to adapt to change… [technology is] changing and changing fast."* – Industry interviewee

Recommended Government Action

OUSW(I&S) should issue implementation guidance (e.g., DOW Memorandum) that DIB companies yet to start the Entity Clearance Determination process will include an ISSM as a required fourth KMP with the same requirements as an FSO and ITPSO (e.g., US-citizen employee). Figure 3 summarizes proposed change. The ISSM KMP would be responsible for the

[55] GSA (2024). *DFARS 48 C.F.R. § 252.204-7012. Safeguarding Covered Defense Information and Cyber Incident Reporting.* Source: https://www.acquisition.gov/dfars/252.204-7012-safeguarding-covered-defense-information-and-cyber-incident-reporting.

[56] DOW CIO (n.d.). *Cybersecurity Maturity Model Certification (CMMC): About.* Source: https://dodcio.defense.gov/cmmc/About/

management and safeguarding of all network environments. Much like the FSO, who is responsible to oversee and manage the physical safeguarding of sensitive and classified information, companies seeking to access and, in some cases, store CUI or classified materials in cyber environments should be required to have the ISSM KMP that can plan, design, implement and attest to safeguarding information security on networks and systems. The requirement creates a predictable baseline for industry to compete for and retain classified work. All DIB companies must demonstrate that cybersecurity is planned, resourced, and led at the same level as physical security.

Within two years of OUSW(I&S) new guidance, companies already possessing Entity Clearance Eligibility should attest and name a cleared individual performing the ISSM KMP role. Non-compliance would reduce a company's Entity Clearance Eligibility to Interim for all new work until the KMP position is filled and attested as required. OUSW(I&S) implementation guidance would serve as a temporary measure pending a broader revision of 32 CFR 117 (NISPOM), a process that may take several years. During a NISPOM revision, Section 117.9 would need to be revised to require four KMPs including the SMO, FSO, ITPSO, and adding the ISSM.

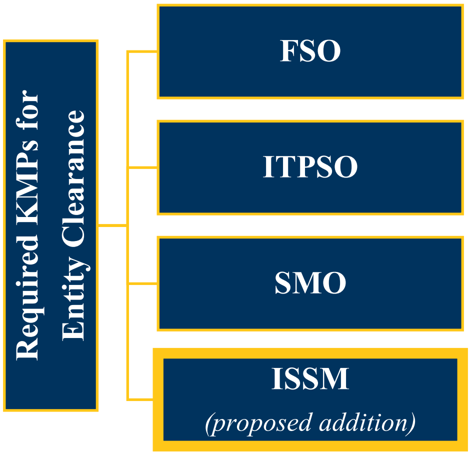
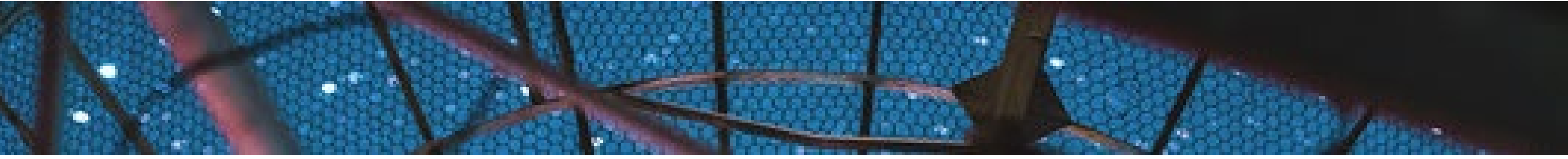


Figure 3. Recommended Required Key Management Personnel (KMP)

Impact for Warfighter

Securing emerging technologies and innovations requires companies to protect not only classified information and networks entrusted to them, but also CUI, intellectual property, prototypes, and software in development. To ensure capabilities reach the warfighter and retain novel battlefield advantage, companies must adopt a proactive cybersecurity posture to prevent adversaries from acquiring these capabilities through malicious means. Elevating an ISSM to a KMP will ensure that the DIB treats cybersecurity as a prioritized part of working with government, and is providing intellectual property to the warfighter that is not already compromised before DOW contracts are even awarded to them. Over time, the alignment is expected to reduce the number of companies with immature cyber postures working on DOW classified work, thereby improving confidence in the integrity and resilience of the DIB delivery to the warfighter.



Cost–Benefit Considerations for DIB Companies

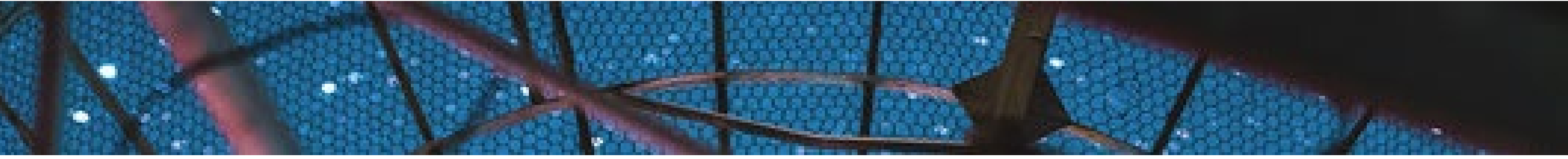
To work on classified contracts, companies would be required to hire or dedicate an employee to the ISSM KMP role. As the recommended government action would uniquely impose a visible, recurring labor expense on industry (rather than just changing government process), the FAST Study team felt it necessary to explicitly outline the cost and offsetting benefits for DIB companies. Industry leaders must be able to justify the ISSM KMP as a new “line-item” expense against the expected costs of cyber incidents, failed or prolonged assessments, schedule delays, and lost contract opportunities. The benefits are expected to cumulatively outweigh the fully burdened cost of the position over the life of a typical classified program, especially for companies that make proactive cybersecurity decisions and investments earlier rather than adjusting or reconfiguring at greater cost later.

For example, the salary for a full-time industry ISSM generally ranges from $119k to $164k.[57] The pay range is significantly outweighed by the average global cost of a data breach: $4.4M.[58] Breaches can also lead to potential repercussions from the federal acquisitions oversight community which could include cancellation of current contracts and debarment from future contracts. In addition, the ISSM role need not be a full-time position, like the FSO and ITPSO roles, and could be combined with other cybersecurity responsibilities at the company until their government classified contract work program expands enough for justified full-time effort. Alternatively, the cyber professional filling the KMP role could be part-time with other companies, reducing the overall cost until contract work expands enough to justify a full-time role.

Requiring an ISSM KMP provides industry with a clear, standardized point of accountability for cybersecurity of government contracts. This role simplifies coordination during cyber assessments, authorizations, and incident response, and reduces reliance on ad-hoc points of contact whose authority and expertise can vary widely. Beyond risk reduction of operational and reputational damage from cybersecurity breaches, it is expected that companies will experience other tangible benefits. These benefits include having fewer unplanned outages from misconfigurations and less failed or prolonged assessments because cybersecurity was not prioritized during early corporate decision-making. The ISSM KMP role is also expected to help companies save money by lowering government’s oversight burden on cybersecurity, and reducing time spent by engineers and program managers on ad-hoc compliance tasks. These efficiencies can offset a substantial portion of the ISSM’s cost by enabling technical staff to focus on delivering innovative capabilities (i.e., working on billable tasks) rather than repeatedly responding to preventable cybersecurity issues.

[57] Salary.com (December 1, 2025). *Information System Security Manager Salary in the United* States. Source: https://www.salary.com/research/salary/position/information-system-security-manager-salary

[58] IBM Security (December 2025). *Cost of a Data Breach Report 2025*. Source: https://www.ibm.com/reports/data-breach



12) Government-Administered SCI Indoctrination Diminishes Project Cost and Efficiency

Challenge

Several industry interviewees, including two councils and consortiums and five larger companies, expressed a renewed desire to conduct Sensitive Compartmented Information (SCI) indoctrinations for their company's employees supporting projects requiring SCI. They reported that, historically, companies with authorized Corporate Special Security Officers (CSSOs) were permitted to perform indoctrination ("read-on") briefings once an employee was approved by the government for SCI access. According to multiple interviewees, this delegated authority was rescinded by DOW, either across the enterprise or within certain MILDEPs. Current practice for these MILDEPs is for personnel to schedule and wait for available SSO government SCI indoctrination briefings. This shift has introduced significant delays as SCI indoctrination appointments are frequently scheduled a week or more after SCI approval and typically conducted at government facilities. As a result, project schedules are extended by weeks, increasing costs associated with underutilized staff awaiting SCI read-ons. When indoctrination briefs are conducted at distant government sites, additional cross-country travel may be required, further unnecessarily increasing labor and travel expenses. Although the SCI indoctrination briefing itself is short and can be organized relatively quickly by security once ready to be scheduled, the administrative steps surrounding it consume disproportionate time and resources. Each year, it is expected that thousands of DIB personnel are indoctrinated into one or more SCI compartments, although no unclassified statistic is publicly available on SCI read-on volume. If it is estimated that 10,000 DIB personnel complete an SCI indoctrination per year, and even a quarter of those had to go through SSO rather than CSSO adding on an average of 5 days waiting, then the DIB loses 100,000 hours of overhead instead of those hours being used to innovate for the warfighter.

The DIB also expressed frustration that this challenge should have already been resolved. In July 2023, OUSD(I&S) issued a memo describing that… "Contractor Special Security Officers (CSSO) may give security indoctrinations for Sensitive Compartmented Information (SCI) via the execution of Form 4414, Sensitive Compartmented Information Nondisclosure Agreement. If delegated the authority by a Government SSO, under a valid contract, the CSSO may execute the form, in coordination with the contractor's contracting officer's representative…" Despite the memo being issued more than two years ago, industry interviewees described SSOs as not being willing to delegate the authority, leading to the aforementioned delays and increased costs.

Recommended Government Action

DOW SSOs should adhere to the OUSD(I&S) July 2023 memorandum, and treat CSSO-administered SCI indoctrination as the default practice subject to limited exceptions. OUSW(I&S) and the Office of the Director of National Intelligence (ODNI) should issue additional guidance clarifying and endorsing the default, routine practice of allowing authorized company CSSOs to conduct SCI indoctrination briefings for their own company's and subcontractor employees approved for project-specific SCI access. The authority for conducting SCI indoctrination briefings should remain with the government Special Security Officers (SSOs), but the *default* position and norm should be that CSSO conduct these briefings for their company's employee with SSOs providing oversight as needed. DODM 5105.21-V1[59] already provides policy endorsement enabling SCI indoctrination briefings to be conducted by the SSO (government) or the CSSO (industry) using standardized DIA produced briefing materials.

Impact for Warfighter

Reaffirming and strengthening DODM 5105.21 guidance, which permits CSSOs to conduct SCI indoctrination briefings under SSO oversight, would result in only marginal risk associated with CSSOs accessing and delivering SCI indoctrination materials and process. In contrast, failing to adopt the recommendation perpetrates the impact of project delays, increases the likelihood of losing subject-matter-experts and other cleared employees, adds costs to industry and government, and may result in solutions less tailored to operational realities of sensitive environments. Implementing the recommendation would improve project efficiency, specifically accelerating timely, cost-efficient and operationally relevant delivery of tailored capabilities and innovations to the warfighter.

13) Prolonged Delays for Additional Entity Clearances Reduces Availability of Classified Facilities

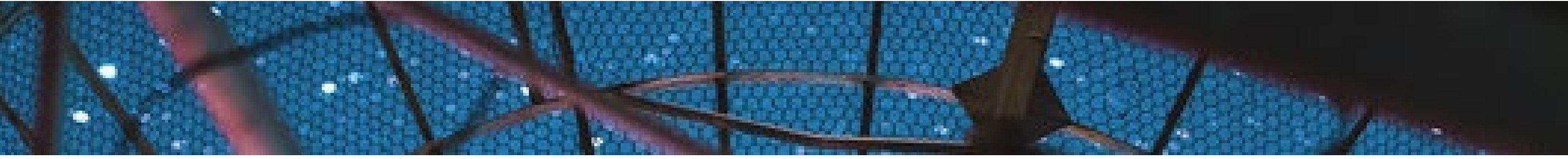
Challenge

Companies that already have an Entity Clearance must submit additional Entity Clearance packages to extend clearances to additional sites[60] or CAGE codes. Multiple interviewees from large companies reported that these submissions are largely duplicative with only minor variations between packages. Approval timelines can vary widely ranging from a few weeks to more than a year. One large DIB company calculated the time required to obtain an Entity Clearance for a new facility after submitting the package was on average a little more than 7 months but ranged from 1 to 17 months. These prolonged timelines are primarily driven by DCSA backlog. Most of these new Entity Clearance packages replicate previously provided and approved information (e.g., business structure, FOCI (and their mitigations), and identify KMPs who already possess PCLs). The duplication in processing increases DCSA workload, exacerbates Entity Clearances backlogs, and delays projects starting work at new locations or for new CAGE codes.

> *"Suggest determining a self-certification authority process by which a company can demonstrate understanding and concurrence with what is needed to implement an FCL, obtain the authority to self-certify branch office FCLs, and then execute quickly with DCSA follow up."* – Industry interviewee

[59] DOD (2020). *DOD Manual 5105.21: Sensitive Compartment Information (SCI) Administrative Security Manual: Administration of Information and Information Systems Security* (Released: 10/19/2012; Appended: 10/6/2020). Source: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/510521m_vol1.pdf

[60] Not to be confused with SCIFs or other sensitive physical area accreditations.



Recommended Government Action

OUSW(I&S) should issue implementation guidance (e.g., DOW Memorandum) allowing trusted DIB companies with proven security records to self-certify additional company sites for Entity Clearance Eligibility. Four industry interviewees at larger companies stated that they wanted the ability to self-certify additional locations and CAGE codes for Entity Clearance Eligibility as a significant advancement to the current process.

For implementation, OUSW(I&S) should define a trusted DIB company as an entity that has maintained an Entity Clearance Eligibility or Access for its headquarters site for more than five years.[61] A "superior rating" in DCSA's Security Review and Rating Process (SRRP)[62] or a determination of Security-in-Depth by the CSA should provide evidence of a company's investment in its security posture.[63] In meeting these requirements, companies may conduct an Entity Clearance Eligibility Self-Assessment for another site or CAGE code within their company. For the DOW, the company would submit:

- Self-assessment
- List of current Entity Clearances already granted to the company
- Security determination evidence:
    - Security Review and Rating Process scorecard provided by DCSA; or
    - Security-in-Depth determination approval letter. Interviewees shared that for DOW these were signed by the local DCSA Field Chief and provided by the DCSA Industrial Security Representatives (ISR). However, it was unclear if they were tracked by DCSA or other CSAs.

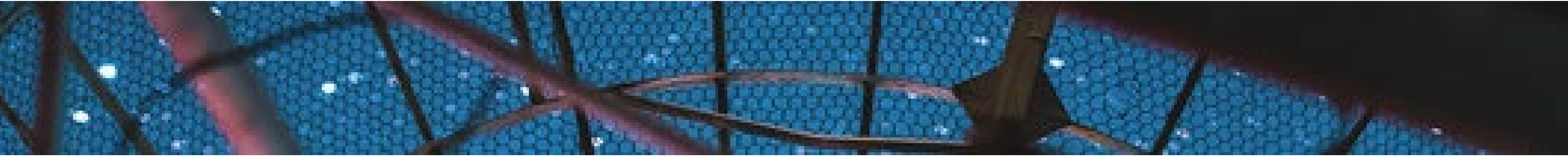
> *"The bulk of classified material sits in our spaces; we are trusted every day to manage that material. Shouldn't we be able to be trusted to maintain self-certifications?"*
> – Industry interviewee
>
> *"The current system strains DCSA resources, creating long delays for approvals. Industry believes "trust but verify" can work, with self-certifications later checked during inspections."* – Industry interviewee

Companies completing self-assessments will be able to operate sites under an *Interim* Entity Clearance Eligibility until a final determination is made by a DCSA audit. The DOW Memorandum should also require DCSA to conduct an audit of the self-assessed site for Final Entity Clearance Eligibility within two years. A DCSA audit of the self-certified Entity Clearance Eligibility with a non-favorable result will suspend entity's ability to conduct self-assessments for

[61] Five years aligns with recommended timeline changes associated with Entity and Personnel Clearance Eligibility administrative terminations and will reflect continued pursuit of classified work and maintenance of clearance.

[62] DCSA (n.d.). *Security Review & Rating Process.* Source: https://www.dcsa.mil/Industrial-Security/National-Industrial-Security-Program-Oversight/Security-Review-Rating-Process/. Note: "Superior" requires companies to conform to a rigorous security posture in four categories: NISPOM Effectiveness, Management Support, Security Awareness, & Security Community.

[63] Government Publishing Office (2025). *32 C.F.R. § 117.3 – Definitions*. Source: https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-D/part-117/section-117.3



five years and will immediately suspend all *Interim* Entity Clearance Eligibility Determinations for the company.

Impact for Warfighter

Allowing DIB companies to self-assess new company sites and CAGE codes for handling classified information (i.e., Entity Clearance) increases efficiency by balancing the trust already provided to those companies with significant deterrents for breaching that trust. This low risk change not only reduces DCSA burden and timelines but also strengthens the partnership between DCSA and companies already proven trusted to safeguard classified materials. Moreover, it incentivizes DIB senior leadership to continue to invest in their security infrastructure and leaders. The self-accreditation process helps enable a subset of companies with demonstrated compliance and security trustworthiness records to begin work earlier, accelerating delivery to the warfighter. This change establishes a graduated incentive for demonstrable advances in security posture, which can increase assurance that the capabilities delivered to the warfighter have not already fallen into the hands of the adversary.

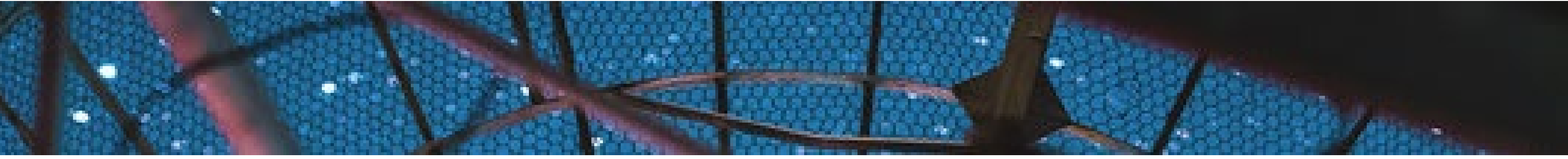
14) Limited Access to SCI and SAP Slots Creates Workarounds

Challenge

DOW limits the number of slots allocated to cleared industry personnel for two different types of positions: (1) technical personnel working on Special Access Programs (SAPs) and (2) corporate overhead personnel working in SCI level programs. While both types of slots require personnel to have a *need-to-know* and *program authority*, technical positions in SAP are tied to specific programs. These SAP slots are typically limited by the type and number of individuals in a specific technical position per contract or program office authority within each of the DOW agencies and MILDEPs.[64] Corporate overhead personnel (i.e., Chief Information Officers (CIOs), contracts, human resources (HR), information technology (IT), and business development (BD)) overseeing SCI level projects for the company are conducting sufficient oversight and meeting business continuity objectives. These SCI slots are tied to specific DOW programs (e.g., Army, Navy) and not specific contracts. Contracting Officer's Technical Representatives (COTRs) control the allocation of these slots.

The DIB described the challenges with the limited number of slots available as twofold. First, the limitation of these slots creates a bottleneck in accessing classified programs for needed technical and business tasks. Contractors are often unable to fully staff projects due to the limitations leaving their employees underutilized, which may require assignment to other tasks. Secondly, DIB companies working on projects that require SCI access often experience challenges in getting enough corporate overhead staff allocated to these slots for proper oversight of these projects and to conduct business and personnel operations.

[64] DOD (2017). *DOD Manual 5205.07, Volume 2: Special Access Program (SAP) Security Manual: Personnel Security*. Source: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/520507v2.pdf



SAP Slot Allocation Limitations

The impact of limited SAP slots to conduct work on SAP projects creates structural inequities across the DIB, adversely impacting small, medium-sized, and large DIB contractors differently. Small DIB contractors face broader consequences when the lack of slots undermines mission readiness and contractor diversity. Small DIB contractors are impacted in the following ways:

- Due to their potential reliance on single SAPs, if slots are unavailable, they are excluded from participating in DOW contracting at this level. Thus, removing their potentially niche expertise and innovative solutions from the DIB.
- Maintaining cleared employees without sufficient slots can be costly and unsustainable.
- Slot shortages can disproportionately block small DIB contractors from SAP level projects, as prime contractors fill slots with their employees first unless government recognizes and advocates for specified allocation.

Medium-sized DIB contractors have more flexibility in the face of limited slots, but are still impacted by having fewer contracts to shift employees onto when these slots are unavailable. The shortage of slots impacts their ability to deliver on contracts, which can lead to loss of follow-on work. It may also limit their competitiveness and ability to scale into a larger DIB contractor.

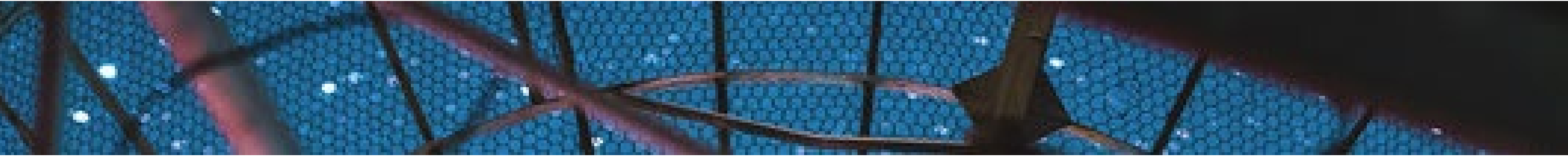
Large DIB contractors experience the least disadvantage from limited SAP project slots as they have multiple contracts where employees can be reassigned while waiting. They are also more easily able to absorb the costs associated with having idle employees. Large DIB contractors can still face delays and loss of efficiency, so they are not completely unaffected when these slots are capped.

Overhead Slot Allocation Limitations

DIB contractors often face difficulties in getting their corporate overhead staff (i.e., Contracts, HR, IT, CIO, BD, Finance) cleared for access to SCI programs. With only a limited allocation of slots available per program, contractors are faced with the decision to allocate limited slots to direct technical staff (e.g., engineers) or those supporting their business continuity (e.g., HR staff, IT personnel). Currently, many DIB contractors describe workarounds such as putting corporate overhead staff onto projects so that they can be cleared. Then, they frequently "read" on and off technical and corporate staff, even weekly, due to the slot allocations. This regular swapping of staff strains resources, delays projects, and does not reduce any risk to the government.

Interviewees highlighted several issues stemming from the shortage of overhead slots:

- Limited access to and availability of business operations positions (e.g., customer contract management, finance, and related support roles) constrains the organization's ability to execute required business processes, degrades customer support, and slows delivery of capabilities to the warfighter, thereby impeding timely mission progress.
- Limited cleared technical staff access hampers continuity by preventing backup coverage during employee departures or illnesses.



- Restricted access to certain RFPs and RFIs limits competitiveness, especially for sub-contracted small companies as prime contractors commonly retain the slots for use by their own company.[65]
- New entrants and small DIB companies are disproportionately impacted in their inability to attend TS//SCI level Industry Days to learn of new opportunities.

> *"[We have a] hard time getting senior leaders read into SCI [slots], so they have oversight. We need more overhead billets for proper oversight."* – Industry interviewee
>
> *"Recommend replacing hard caps for SCI* [slots] *billets with an accountable risk owner managing the dynamic access. Also, create non-encumbering* [slots] *for required back-office roles."* – Industry interviewee

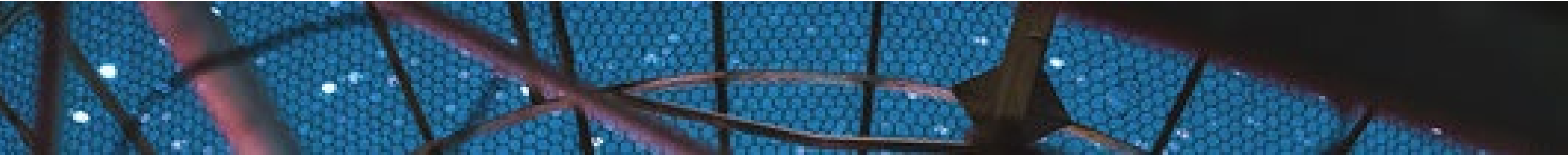
Recommended Government Action

The DOW should adopt a risk-based approach to slot allocation, moving from a rigid slot caps system to a framework that balances mission need, operational continuity, and security risk. Interviews with DIB leaders and innovators yielded the following recommendations:

- Utilize temporary "surge slots" with approval from the KO or Contracting Officer in Chief (CoCO)[66] to address times of critical need.
- Consider allocating slots as a percentage of each company's total number of cleared personnel, to promote an equitable distribution between small and large DIB companies and to ensure that small DIB companies are not disproportionately constrained by a fixed, low number of slots relative to their business and corporate overhead staffing needs.
- Create tiers of slots to ensure that small businesses and subcontractors are not disproportionately excluded from SCI opportunities (i.e., continuity-critical, mission-essential, and competitive-access tiers).
- Ensure sufficient allocation of business operations positions (e.g., customer contract management, finance, and related support roles), recognizing them as mission-critical enablers of customer support. Limiting access to or availability of these slots constrains the capacity to execute required business processes, slows delivery of support to the warfighter, and impedes timely mission progress.
- Establish rotational or shared slots for corporate overhead staff supporting business continuity (i.e., CIO, HR, IT, BD) to reduce the number of permanent slots that are needed while still mitigating continuity risks.
- Use auditing, enhanced monitoring, and training for slots that are deemed higher risk.

[65] See *Lack of Co-Use Spaces for Classified Proposal Development Restricts Competition*

[66] Defense Acquisition Regulations Supplement (DARS). *5817.202-90 User of Surge Options*. Source: Acquistion.GOV. https://www.acquisition.gov/dars/5817.202-90-use-surge-options



- Use data-driven oversight, such as tracking slot utilization and measuring risk outcomes around continuity gaps, security incidents, and missed opportunities allowing for dynamic adjustment of SCI and SAP slots versus relying on static slot caps.

The biggest recommendation to government is to allow contractors to assess and provide a justification for the number of slots they believe are reasonably needed to do the work for both technical and overhead tasks.

> *"It's a business enabler… lose it and you're hurt. So, we protect it."* – Industry interviewee

Based on these recommended changes, SAP slot allocations should be addressed by OUSW(I&S). OUSW(I&S) should update the DODM 5105.21[67] to incorporate risk-based approaches. In turn, each MILDEP should update its service-level implementation guidance accordingly.[68,69] Limitations in allocated SCI slots, particularly for corporate overhead staff, should be addressed by OUSW(I&S) via updates to the latest version (Volume 3) of the DODM 5105.21 in collaboration with the DIA, as the DOW functional manager for SCI.[70]

Impact for Warfighter

Implementing these recommended changes will yield significant benefits for the warfighter. First, they expand DOW's access to innovation by increasing small and medium business participation in SCI and SAP level contracts and programs. Second, they accelerate the delivery of cutting-edge technology to the warfighter by preventing the current read-on and off swap happening today. Finally, they reduce disruptions to mission-critical programs by minimizing missed opportunities for system and product upgrades, or other customer supports, that delay program execution through improved access to needed slots to successfully perform.

15) Lack of Personnel Clearance Reciprocity Increases Cost and Delays DIB Support to Warfighter Missions

Challenge

FAST Study interviewees consistently described weak reciprocity in personnel security clearances as a central obstacle to DIB being able to provide rapid innovation to warfighter missions (as well as to broader USG missions). Existing policy and guidance are supposed to enable broad reuse of prior clearance decisions. For example, NISPOM repeatedly requires CSAs to acknowledge and

[67] DOD (2012). *DOD Manual 5105.21, Volume 3: Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Personnel Security, Industrial Security, and Special Activities* (Incorporating Change 2, September 14, 2020). Source: https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodm/510521m_vol3.pdf

[68] DOD (2012). *DOD Manual 5105.21, Volume 3: Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Personnel Security, Industrial Security, and Special Activities* (Incorporating Change 2, September 14, 2020). Source: https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodm/510521m_vol3.pdf

[69] Service-level implementation guidance includes documents: Army Regulation (AR) 380-28 *Army Sensitive Compartmented Information Security Program;* Secretary of the Navy Instruction (SECNAVINST) 5510.30C *Department of the Navy Personnel Security Program*; Marine Corps Marine Administrative Message (MARADMIN) 165/24 *Sensitive Compartmented Information Security Program Establishment Process, 2024*; and Air Force Manual (AFMAN) 16-1405 *Air Force Sensitive Compartmented Information Security Manual.*

[70] DOD (2013). *DOD Manual 5105.21, Volume 3: Sensitive Compartmented Information (SCI) Administrative Security Manual: Volume 3, Physical Security* (Incorporating Change 2, September 8, 2017).

accept personnel clearances.[71] SEAD-7[72] further requires agencies to accept background investigations and national security adjudications at the same or higher level unless an update is required or the Security Executive Agent (SecEA) specifically approves additional investigative or adjudication requirements. However, the FAST Study interviewees repeatedly described a lack of reciprocity not only between CSAs (e.g., DOW to IC) but also within departments/agencies of a CSA (e.g., Army to Navy, CIA to NRO). In practice, departments/agencies frequently add their own processes on top of shared standards. Interviewees reported that DIB personnel who already hold an active clearance and are enrolled in continuous vetting are often subjected to new, department/agency specific checks before another organization recognizes their personnel clearance eligibility. Though the focus of the FAST Study is on DOW challenges, this challenge is present across USG; interviewees also described similar challenges with other departments such as the Department of Energy (DOE) and Department of Homeland Security (DHS).

The impact is that a PCL granted and maintained under one agency's authority is not reliably accepted by another, even when the underlying investigative standards are the same. While TW 2.0 initiatives continue to standardize and improve requirements, there is still more work to be done. Industry interviewees emphasized that the uneven implementation of TW 2.0 initiatives are resulting in extended project timelines, increased costs, and staff shortages. Many of the costs are incurred while new hires wait on national security clearance adjudication or duplicated background investigations for additional agency-required, non-standardized investigative elements (e.g., different polygraph standards and requirements between agencies).

One visible impact is the unpredictable and wide range of timelines reported by DIB for gaining access based on an existing clearance eligibility. Some departments/agencies are able to complete a basic crossover in a matter of days once they verify the person's eligibility and continuous vetting status. Others take months to complete essentially the same action, even when there is no new derogatory information. DIB interviewees described people waiting months to more than a year to be brought on to support a mission in a new department/agency despite having current eligibility.

Other interviewees mentioned that the disconnect could even be observed for individuals in the same position depending on how they were assigned (i.e., Temporary Duty Assignment, Permanent Change of Station, Systems Engineering and Technical Assistance (SETA) contract, direct hire). For example, interviewees recounted situations where the same person, doing essentially the same work on the same systems, could start almost immediately if they moved through one hiring or contracting path, but faced months of delay if they entered through another. In these cases, the variation was driven by internal process choices, not by differences in the person's background or risk profile.

Polygraph practices compound the problem. Personnel who have completed a polygraph for one IC element are often required to undergo additional polygraphs when moving to another, even

[71] 32 CFR 117.10(h). Source: https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-D/part-117/section-117.10

[72] ODNI (2018). *Security Executive Agent Directive 7 (SEAD-7): Reciprocity of Background Investigations and National Security Adjudications.* Source: https://www.dni.gov/files/NCSC/documents/ Regulations/SEAD-7_BI_ReciprocityU.pdf

when the access requirements are very similar. These extra examinations add time and cost without necessarily providing new insight into risk.

The challenges described affect government civilians and service members, but the burden on the DIB is particularly acute. DIB companies often support multiple departments/agencies and rely on being able to move cleared employees between programs to meet changing operational needs, share expertise, and manage costs. Those same employees can facilitate collaboration across MILDEPs and the USG, which reduces costs for spreading innovation and reusing taxpayer-funded DIB-built capabilities. As clearances are not yet genuinely reciprocal, companies cannot easily redeploy personnel to where the warfighter and mission need them most. DIB employees can sit idle waiting for new adjudications, while other projects remain understaffed. Over time, some cleared professionals shift to jobs that do not require a clearance to avoid extended downtime and uncertainty, shrinking the pool of DIB talent available to innovate the warfighter's advantage on the battlefield.

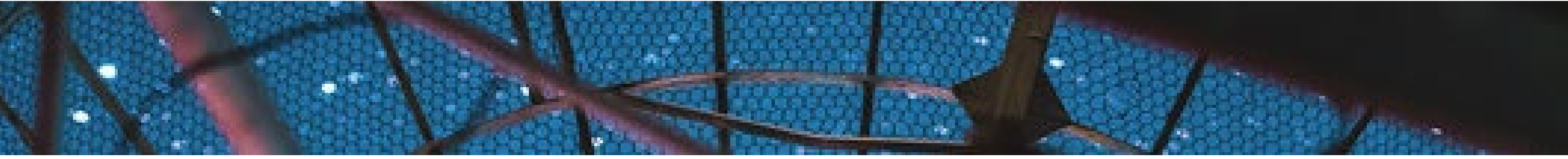
Recommended Government Action

The USG should accept reciprocity in personnel clearances as a requirement for mission success and enforce it using existing authorities and the reforms underway through TW 2.0. ODNI (in its role as SecEA) in coordination with OPM, DCSA, and the other CSAs, should establish a single, integrated framework for PCLs and adjudications that all IC and DOW components are required to follow. The framework should cover standards for investigations, adjudications, continuous vetting, and polygraph practices. Any deviations should be rare, justified in writing, and tied to clearly defined mission needs, rather than historical habits or individual agency preferences. Within that framework, national security clearance eligibility should be treated as fully portable across departments/agencies.

Polygraph practices should be aligned in support of reciprocity. Departments and agencies should work through ODNI to harmonize polygraph procedures, including formats, quality control, and how inconclusive results are handled. Once common standards are in place, agencies should accept polygraph results for the same general level and type of access. Additional testing should be limited to clearly defined, risk-based situations.

Eligibility should be treated as a shared, government wide decision. *See Conflation of National Security and Suitability/Fitness Adjudications Impedes Reciprocity* for actions DOW would need to take to contribute to true reciprocity. However, understandably, suitability and fitness decisions may differ by mission and role but should not be used as a reason to re-adjudicate all eligibility and access determinations. Policy, systems, and training should reinforce this distinction so that agencies make appropriate, role-specific judgments while honoring clearance eligibility granted elsewhere.

Lastly, the DIB requested in the FAST Study that ODNI lead the way toward USG enterprise-wide personnel clearances security training and reporting requirements. Where content and frequency are effectively the same, departments/agencies should recognize training completed for another agency, and should not require DIB employees to repeat near identical courses simply because they change the MILDEP they are focused on. Reporting obligations such as foreign travel or



foreign contact reporting should be aligned as far as possible to minimize DIB employees having to duplicate reporting the same information.

Impact for Warfighter

Persistent gaps in reciprocity for personnel clearances slow down the movement of experienced DIB SMEs to priority missions. When individuals who already hold clearances and are enrolled in

continuous vetting no longer have to wait months for a department/agency to recognize their eligibility nor complete duplicative steps, the warfighters operate sooner with needed expertise, new capabilities, and critical surge responses.

For the DIB, the cost savings from not having to carry personnel required for contracts yet cannot start work is significant. The impact will be particularly felt by small companies and NDCs that support multiple agencies who will not have to absorb long periods of non-billable time. Over time, more reliable reciprocity will lower cost, reduce frustration for cleared personnel, and make cleared work more attractive to innovative companies and individuals. This, in turn, will expand the pool of talent and ideas available to support warfighting and defense missions and increase the speed at which new capabilities reach the field.

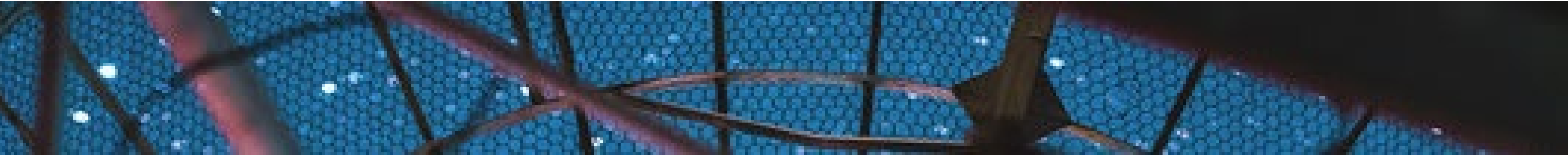
16) Terminology Ambiguity in *Personnel Clearances (PCL)* Reduces Onboarding Readiness

Challenge

Use of the ambiguous term *Personnel Clearance (PCL)* blurs the distinction between eligibility and access to national security classified information. FAST Study interviewees from small businesses and NDCs, and their management who are new to PCLs, are unclear as to the distinction when assigning personnel to classified projects, particularly when those personnel must be "read-on" to have access to the classified information and/or enrolled in continuous vetting (CV).[73] Distinguishing between PCL eligibility and access becomes even more challenging when personnel move between DOW, Intelligence Community (IC), and other federal agency projects. Both government and industry sometimes conflate PCL adjudications as meaning *both* an individual's ability to access national security classified information and the acceptance of risk associated with position assignment (i.e., suitability/fitness). The FAST Study found that this latter challenge creates interagency reciprocity issues and confusion in industry regarding who can access classified information and who can fill specific positions (a challenge addressed in greater detail in the next recommendation[74]). Ultimately, clarifying the terminology associated with PCLs will reduce confusion and frustration over why an eligible individual may not immediately be able to access classified information, and should improve reciprocity among Cognizant Security Agencies (CSAs).

[73] CV enables ongoing checks for security-relevant information. Enrollment in CV only occurs when PCL eligible and affiliated with the Federal Government.

[74] See: *Recommendation 2) Conflation of National Security and Suitability/Fitness Adjudications Impedes Reciprocity*



Recommended Government Action

DCSA should issue guidance that the term *PCL* must be used in conjunction with the terms *Eligibility* or *Access* in the future to specifically designate an individual's national security clearance status and specify their current access to classified information and enrollment in CV. Accordingly, the term ***Personnel Clearance-Eligible*** (and subsequently Secret-Eligible and Top Secret-Eligible) should be used to indicate an individual has been investigated and adjudicated as trustworthy to the U.S. and is granted the ability to safeguard classified information. Alternatively, when an individual is adjudicated for a specific position (e.g., Military Occupational Specialty (MOS)), and is indoctrinated (i.e., "read-on") to a program the term ***Personnel Clearance-Access*** (and subsequently Secret-Access and Top Secret-Access) should be used. Table 4 provides an overview of the changes, including example definitions to describe the distinctions between Eligibility and Access.

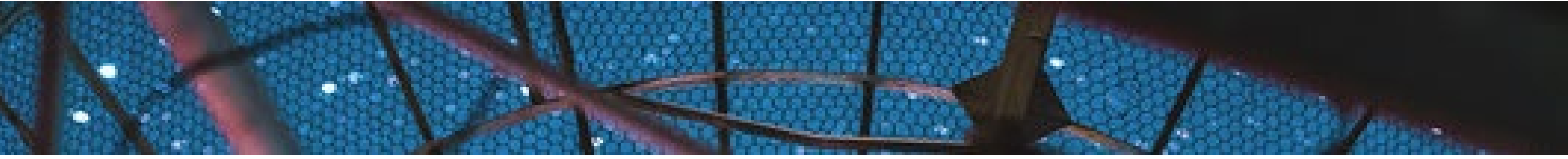
Table 4. Personnel Clearance Terminology and Acronyms

Current Terminology	Proposed Terminology
Personnel Clearance (PCL)	**Personnel Clearance – Eligible (PCL-E)** Individual has been investigated and favorably adjudicated to a specific clearance level, suggesting they can safeguard national security information to the level of clearance
	Personnel Clearance – Access (PCL-A) Individual has been favorably adjudicated as suitable/fit to be in a position, determined to have a "need to know," and read-on to classified project work at or below their clearance level[75]

Impact for Warfighter

Specifying *Eligibility* and *Access* as the terms used to describe an individual's clearance status will help elucidate reciprocity among CSAs, with a goal of more efficient information sharing and protection across DIB, government missions, and the warfighter. Distinguishing between *Eligibility* and *Access* helps the government differentiate between individuals enrolled in CV and those who may need investigative updates (e.g., record checks, interviews) before being allowed to access classified information. Additionally, clarifying PCL terminology should reduce confusion about who has access to information and prevent potential classified information spills. Unintentional spills can occur when an individual in access provides classified information to someone who is eligible but does not have access. Ultimately, using clear and complete terms will facilitate reciprocity between CSAs, help safeguard national security information, and more rapidly deliver new and innovative technologies to the warfighter.

[75] The White House. *Executive Order 12968—Access to Classified Information [Section 1.2]*. Source: https://www.govinfo.gov/content/pkg/WCPD-1995-08-07/pdf/WCPD-1995-08-07-Pg1365.pdf



17) Misaligned Entity and Personnel Clearance Eligibility Timeframes Reduce DIB Availability

Challenge

32 CFR 117 is the federal rule governing Personnel Clearance[76] and Entity Eligibility Determination (hereafter Entity Clearance),[77] providing the requirements for obtaining, maintaining, and terminating eligibility and access to national security classified information. This section focuses on the termination of eligibility for personnel and entities which are not equivalent in the federal rule.

DODM 5200.02 allows personnel with a favorable adjudication for a national security investigation with a break in service to maintain their PCL *eligibility* and return to *access* for up to two years.[78] Since then, TW 2.0 initiative established continuous vetting (CV) in which information is collected from records checks and mission partners to ensure government and DIB personnel continue to safeguard people, property, information, assets, and mission. TW 2.0 also permits the transfer and re-establishment of trust after a break in service if the individual satisfies standards to access classified information.[79] This TW 2.0 revision suggests that PCL eligibility is not administratively terminated but would just require updated investigative checks to re-establish the baseline of trust.[80] Government interviewees clarified that individuals who held PCL *eligibility* and were affiliated[81] with the Federal Government were enrolled in CV.[82] However, when an individual experiences a break in service (i.e., is unaffiliated with the Federal Government), they are unenrolled from CV but maintain their PCL *eligibility.*[83]These individuals may require additional investigative checks to re-establish a new baseline of trust. The number and type of investigative checks will depend on how long they have been unaffiliated and any risk tolerance difference between new position requirements and their PCL status at the time affiliation lapsed (e.g., difference in investigative tier or position-specific requirements). Interviewees stated that the eligibility period while unenrolled from CV could currently last five years before returning to PCL access would require a full reinvestigation and adjudication.

Compared to PCL *eligibility*, the CFR does not specify a timeframe for Entity Clearance Eligibility administrative termination. Instead, the CFR describes that there can be termination because the company does not have or has not pursued classified work. CDSE *Facility Clearances in the NISP*

[76] Government Publishing Office (2025). *32 C.F.R. § 117.10 – General requirements*. Source: https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-D/part-117/section-117.10

[77] Government Publishing Office (2025). *32 C.F.R. § 117.9 – Reporting requirements*. Source: https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-D/part-117/section-117.9

[78] DOD (2017). *DOD Manual 5200.02: Procedures for the DOD Personnel Security Program (PSP)* (Incorporating Change 1, October 29, 2020). Source: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/520002m.pdf

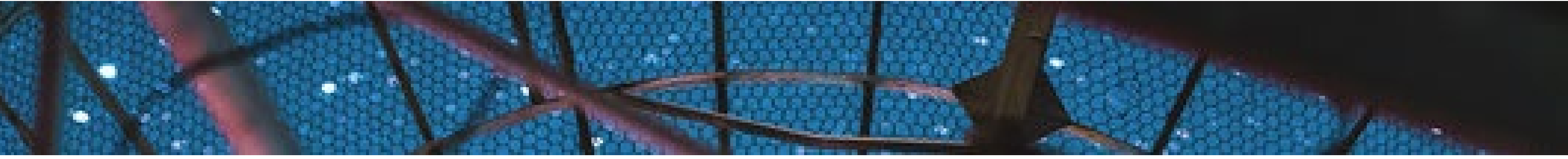
[79] ODNI & OPM (2025). *Memorandum: Trusted Workforce 2.0 Implementation and Operational-Level Guidance for Departments and Agencies and Authorized Investigative Service Providers – Upgrades, Transfer of Trust, and Re-establishment of Trust Vetting Scenarios.*

[80] ODNI & OPM (2022). *Federal Personnel Vetting Guidelines.* Source: https://www.dni.gov/files/NCSC/documents/Regulations/Federal_Personnel_Vetting_Guidelines_10FEB2022-15Jul22.pdf

[81] Individual who holds PCL initially affiliated with Federal Government agency and therefore immediately enrolled in CV when granted PCL.

[82] ODNI & OPM (2025). *Memorandum: Federal Personnel Vetting Management Standards*.

[83] CV requires that an individual only provide products or services to their affiliated government agency but does not specifically require PCL eligibility. Case in point, individuals in non-sensitive public trust or low risk positions are enrolled in CV but do not have a PCL.



Student Guide[84] states Entity Clearance Eligibility should be administratively terminated after a company fails to provide evidence of government classified procurement activity or classified work in the past 12 months, with no reference to any authoritative source for that guidance. Unclear guidance on administrative termination of Entity Clearance Eligibility causes challenges for small and medium companies which have successfully finished a classified project but are not a fit for current classified opportunities. In addition, misaligned timeframes for PCL Eligibility and Entity Clearance Eligibility creates unnecessary confusion and complexity for industry, and for the DCSA in tracking alignment.

> *"If you had an FCL three months ago and the same cleared KMPs [Key Management Personnel], why [do we need to] start over?"* – Industry interviewee
>
> *"It depends on the ISR [Industrial Security Representative]. It is dependent upon regions. One [ISR] may say that they are good to give you additional time and another may say that the FCL will be terminating in 30 days."* – Industry interviewee

Recommended Government Action

OUSW(I&S) should develop and release clarifying guidance (e.g., DOW Memorandum) specifying PCL Eligibility and Entity Clearance Eligibility will require a full background investigation and investigation after five years' break in service. For PCLs, administrative termination from *eligibility* would be extended from DODM 5200.02[85] to occur five years after the individual is no longer affiliated with a Federal Government agency and has been unenrolled from CV. During this five-year period, individuals would still maintain PCL Eligibility and would need updated records checks and review of any changes to the Personnel Vetting Questionnaire (PVQ). After a break in service of more than five years, PCL Eligibility will be administratively terminated, and individuals will require a new full background investigation and adjudication to return to eligibility and/or access. The current action for PCLs would extend the current DODM 5200.02 and reiterate TW 2.0 guidance for requiring a full background investigation and adjudication to five years, which would clarify and standardize the PCL Eligibility timeframe. PCL Access timeframes would remain unchanged as they are only terminated when *need to know* is no longer required.

Clarifying and standardizing PCL eligibility timeframes between DODM 5200.02 and TW 2.0 guidance would benefit the DIB by extending access for military veterans separating from service and entering industry. Additionally, it would permit cleared individuals tasked to non-classified projects to return to classified positions and projects allowing them to continue to support the mission. It also reduces DCSA's PCL backlog and cost of redoing initial background investigations and adjudications.

[84] CDSE (2022). *Facility Clearances in the NISP IS140v4: Student Guide*. Source: https://www.cdse.edu/Portals/124/Documents/student-guides/IS140-guide.pdf

[85] DOD (2020). *DOD Manual 5200.02: Procedures for the DOD Personnel Security Program (PSP). Section 4.1(b)(2), Section 4.2(c), Section 5A.3(e), and Section 7.14(b).* Source: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/520002m.pdf

Administrative termination timeframes for Entity Clearance Eligibility should also be set for five years after the company has not pursued or performed classified work. During this interval, the entity can maintain its Entity Clearance Eligibility by updating its NISS account for all change conditions. Companies that are Entity Clearance Eligible, but not in *access* should attest annually to pursuit of classified work as evidenced by proposal confirmation to a solicitation for classified work. Companies unable to provide this evidence while in eligibility will be administratively terminated after five years. After this administrative termination, companies would be required to go through the Entity Eligibility Determination process for a new Entity Clearance to return to eligibility and access. This change would clarify the timeframes and requirements for Entity Clearance Eligibility. Additionally, the longer window would maintain an expanded pool of companies able to bid and perform classified work while limiting Entity Clearances to companies interested or involved with classified projects for the government and who are maintaining their security posture.

Impact for Warfighter

Aligning and extending PCL and Entity Clearance administrative terminations timeframes to five years will enable DOW to maintain a significantly larger DIB, while also rapidly allowing personnel and companies to return to access in support of the DOW mission after time away (e.g., retirement from government, career change, secondment). These actions will reduce burden for companies, individuals, and DCSA while still managing risk through required updates from companies via submission of change conditions and from individuals through updates to investigations (before re-enrolling in CV). It will also reduce delays and rework as *eligibility* is maintained for a longer timeframe and can restart *access* more quickly. Overall, aligning PCL Eligibility and Entity Clearance Eligibility timeframes reduces confusion across the government and DIB and more importantly reduces barriers for re-entering classified contracting for small, medium, and nontraditional companies. Finally, this alignment makes classified contracting more attractive to both companies and individuals, which in turn enables a wider set of innovative options for the warfighter to rely on for battlefield advantage.

18) Conflation of National Security and Suitability/Fitness Adjudications Impedes Reciprocity

Challenge

In 2022, TW 2.0 Federal Personnel Vetting Guidelines[86] reduced the number of investigation tiers from five tiers to three, collapsing Tiers 2–3 into the Moderate Tier and Tiers 4–5 into the High Tier. The revision aligned national security investigation and adjudication with similar risk-based public trust suitability and fitness adjudications,[87] and simplified the vetting process. According to a government interviewee, DOW, to date, uses National Security clearance adjudications not only to assess loyalty and risks associated with access to classified information but also as a proxy

[86] ODNI & United States Office of Personnel Vetting (2022). *Federal Personnel Vetting Guidelines*. Source: https://www.dni.gov/files/NCSC/documents/Regulations/Federal_Personnel_Vetting_Guidelines_10FEB2022-15Jul22.pdf
[87] CDSE (2024). *Federal Personnel Vetting Investigative Standards Short*. [Student Guide]. Source: https://www.cdse.edu/Portals/124/Documents/student-guides/shorts/PSS0111-guide.pdf

for evaluating individual's conduct and character risks for a specific position. While the assumption that national security clearance adjudications can subsume suitability and fitness adjudications, it both increases risk to the safeguarding of classification and impedes the rapid transition of those departing the military into the DIB.

The IC and other federal agencies typically adjudicate for position suitability and fitness and, when needed, for national security. DOW's reliance on national security adjudications as a proxy for position suitability and fitness determinations has created reciprocity challenges with these federal agencies. The IC/other federal agencies, which adjudicate for position suitability and fitness, frequently require additional investigation and adjudication actions (e.g., polygraph) whenever personnel are assigned to IC or other federal positions, or when recently separated military members are hired into DIB companies to support the warfighter mission. For example, when an individual separates from the military and becomes a DIB contractor to the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF), reciprocity does not apply and their hiring is delayed by conducting a suitability and fitness adjudication.

Currently, military recruits are onboarded and most are investigated and adjudicated for Secret Clearance eligibility (e.g., at Basic Training or Officer Candidate/Training School). The current DOW process is to only adjudicate for national security and not suitability/fitness. Once granted eligibility they may be reassigned or request a different MOS. Within military commands, those with clearance eligibility may be 'read-on' to access mission information at their clearance level without any adjudication of their suitability (i.e., conduct and character risks) for the position. This practice leads to assignments where conduct risks are not fully considered, for example, placing an individual with a history of substance misuse in a medical role with access to controlled substances, thus increasing insider threat risk. Although it is expected that individuals with a history of substance misuse can be identified and steered away from MOSs that may be challenging for them, this does not often occur. As a result, military personnel entering the DIB reasonably believe they are eligible and suitable based on their previous favorable national security clearance eligibility. They experience considerable frustration and DIB project hiring and/or execution are delayed until those previous servicemembers are adjudicated for suitability.

Recommended Government Action

DOW should disaggregate the national security clearance adjudication from position adjudication (e.g., MOS) for its military, civilian, and contractor personnel. This process would require that national security adjudications remain the purview of DOW Consolidated Adjudications Facility (CAF) for determination of *eligibility* to handle classified information but would require DOW programs, MILDEPs, agency personnel security offices, or other authorized officials to adjudicate personnel for their position. Acknowledging that this process would initially increase the workload of these authorizing officials during MOS changes, it would increase reciprocity between DOW, IC, and other federal agencies. Adjudications for more granular position changes (e.g., assignment to new duty stations within current MOS, promotions) were considered, but it was unclear whether the return-on-investment would be beneficial. During data collection, the FAST Study learned that DOW was beginning to implement position suitability/fitness adjudications for some more sensitive positions. The FAST Study recommends continuing to expand the initiative across the DOW after initial implementation.

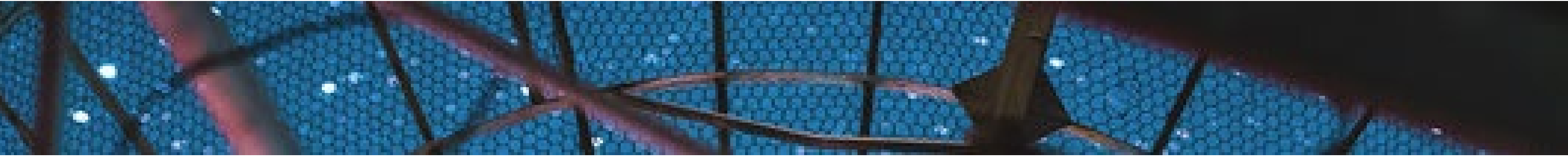
Impact for Warfighter

Disaggregating national security and suitability/fitness adjudications will benefit not only DOW but the whole of government. From a risk management perspective, this approach lets DOW investigate and adjudicate national security clearance eligibility quickly by determining whether an individual can handle classified information at the required level while also recognizing that standards of conduct and character requirements vary by position (i.e., job roles, MOS) under suitability/fitness criteria. Thus, an individual may be appropriate to handle classified Secret logistical information related to food supplies or truck parts, but they may not be best suited to handle classified Secret information associated with drug shipments or regional mission planning.

When military servicemembers move into the DIB usually filling similar positions, disaggregation will strengthen reciprocity between DOW, IC, and other CSAs, easing transitions for military veterans and other cleared government personnel into the DIB. Facilitating their move from government service into the DIB enables those who understand the mission to more easily remain engaged and continue in industry to support the mission and warfighters.

ENTITY ELIGIBILITY AND ACCESS INDUSTRY CHALLENGES

1. Lack of DCSA Problem-Solving and Connection to Warfighter Mission Reduces Security Enterprise Urgency
2. DCSA Inconsistencies in Guidance and Decisions Delays Projects and Fosters DIB Frustration
3. Facility Clearance Terminology Impedes DIB Entry
4. Lack of Entity Clearance Eligibility Sponsorships Creates Barriers to Entry
5. Complexity in Preparation of DD Form 254 Hinders DIB Expansion
6. Lack of Automation and Tools Hinders Faster Entity Clearance Package Reviews
7. NISS Change Conditions Cause Holds, Creating Unnecessary Risk
8. Outdated Facility Clearance Orientation Handbook Increases Subcontractor Confusion
9. DOD Enhanced Security Program Underutilization Reduces Innovative Problem-Solving
10. Lack of Co-Use Spaces for Classified Proposal Development Restricts Competition
11. Cybersecurity is Not a Required Key Management Personnel Role, Leading to Systemic Technical Risk
12. Government-Administered SCI Indoctrination Diminishes Project Cost and Efficiency
13. Prolonged Delays for Additional Entity Clearances Reduces Availability of Classified Facilities
14. Limited Access to SCI and SAP Slots Creates Workarounds
15. Lack of Personnel Clearance Reciprocity Increases Cost and Delays DIB Support to Warfighter Missions
16. Terminology Ambiguity in Personnel Clearances (PCL) Reduces Onboarding Readiness
17. Misaligned Entity and Personnel Clearance Eligibility Timeframes Reduce DIB Availability
18. Conflation of National Security and Suitability/Fitness Adjudications Impedes Reciprocity



FOREIGN OWNERSHIP, CONTROL, OR INFLUENCE (FOCI)

Across industry interviewees, FOCI was not consistently viewed as a primary barrier to entry in working with the USG. With mitigations, the presence of FOCI does not prevent companies from working with the DOW. Overall, interviewees representing both non-FOCI and FOCI-mitigated companies recognized risks posed by FOCI and the importance of accompanying reviews and mitigations. Findings indicate the FOCI process and requirements should not be reduced but be made more efficient and flexible to address risk and implement mitigations at speed of mission.

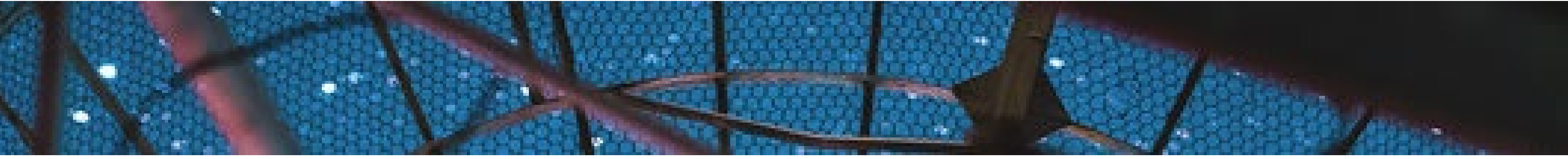
FOCI-mitigated companies are a small yet critical group. Per a FOCI subject-matter-expert interviewee, approximately 3% of the 10,000 NISP cleared entities are FOCI-mitigated. The FAST Study team collected data from 21 companies/individuals with FOCI expertise, including 11 FOCI-mitigated companies (security leadership and practitioners), 6 security integrators for FOCI companies, 3 lawyers with FOCI expertise, and 3 security practitioners with previous FOCI experience. Table 5 provides an overview of the challenges raised. Interviewees from FOCI-mitigated companies highlighted common challenges and disadvantages due to FOCI status, which impacts cost, time, performance, and competition. As USG prepares to implement Section 847 of the FY20 NDAA, henceforth referred to as Section 847, more companies will undergo FOCI review and the number of companies in the FOCI-mitigated group will expand. Consequently, now is the critical time to examine the FOCI process, prioritize areas for action, and deliver change.

Table 5. FOCI Challenge Area Overview

	Challenge Area
FOCI Review Process	1. SF-328 complexity and inefficiency 2. Understanding the new SF-328
FOCI-Mitigated Company Experience	3. Negative perceptions 4. Delays 5. Ineffective use of ODs and GSCs
Supplemental FOCI Documentation	6. Need for modernized ECP 7. Burdensome AOP 8. Outdated templates and guides 9. ECP and CMMC overlap
Modernizing the FOCI Approach	10. Current FOCI approach outdated
NDAA Section 847	11. $5M threshold remains undefined 12. Implementation guidance critically needed

Impacts for Warfighter for all FOCI recommended government actions

By addressing all of the FOCI challenges and recommendations in this focus area, DOW will enable both new and existing FOCI-mitigated companies to start work faster, resulting in more efficient delivery to the warfighter. Earlier delivery of innovative solutions, developed from the ingenuity of the DIB, will maintain and widen the warfighter's battlefield advantage.



DOW can further attract and leverage key innovation from FOCI-mitigated companies through addressing inefficient and burdensome processes, and correcting negative perceptions of FOCI-mitigated companies. However, it is critical that FOCI processes be strategically rather than incrementally modified to protect the warfighter's battlefield advantage. Ultimately, the warfighter must be able to rely on and trust that the capabilities delivered by the DIB are protected against foreign adversaries skillfully exploiting FOCI leverage over DIB companies. Maintaining a streamlined yet rigorous FOCI process is essential to assure provenance, prevent covert influence, and safeguard mission outcomes.

FOCI Review Process

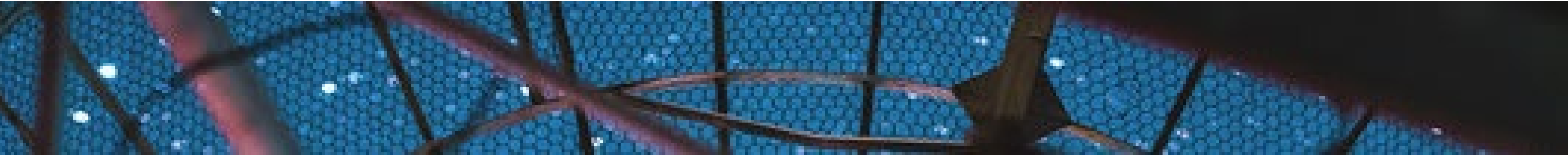
All companies pursuing or maintaining an Entity Clearance Eligibility must complete a FOCI review. During interviews, feedback on the FOCI review process centered around the Standard Form 328 "Certificate Pertaining to Foreign Interests" (SF-328), and coordinating with DCSA.

19) SF-328 Complexity and Inefficient Review Process

Challenge

Based on FAST Study data, extensive information identification and gathering burden, and the time to manually complete the form, particularly for small businesses and NDCs are the primary challenges with the SF-328. This process typically requires many months to a year of effort. By the time DCSA's review of the company's submitted SF-328 is finalized, business changes often necessitate revising content or submitting change condition packages. Gathering the highly-detailed information involves coordination between security, legal, finance, and other departments, subsidiaries, investors, suppliers, and parent organizations. Data collection for the SF-328 is especially challenging with foreign entities that must adhere to differing foreign reporting standards and privacy laws. Gathering the information for the SF-328 requires significant corporate overhead involvement and often necessitates hiring costly legal counsel with FOCI- and DCSA-specific knowledge and experience.

Industry described the SF-328 review process with DCSA as inefficient, commonly involving back-and-forth communications to address changes and clarifications, and lengthy periods of no DCSA response. Based on study data, the process from SF-328 submission to final approval takes 40 weeks on average. As one Security-as-a-Service provider described, *"the SF-328 typically gets rejected regardless of what you submit."* Furthermore, upon an incomplete or deficient second submission, a company is placed at *"the back of the line"* by DCSA. Three interviewees noted the process from submission to approval took approximately two years, describing that their companies did not receive requests for more information from DCSA until one year after submission. Consequently, the FOCI review process delays companies from obtaining their Entity Clearance Eligibility, starting work, and delivering innovative capabilities to the warfighter. Given delays and frequent returns for clarifications, the SF-328 and FOCI review process must be addressed by DCSA.



Recommended Government Action

With the frequency at which the SF-328 is returned to industry for clarifications, and the length of time industry needs to gather information to respond, the FAST Study recommends DCSA implement a more efficient automated error check to triage the SF-328 information. During data collection, the FAST Study team became aware of DCSA efforts to modernize the NISS and plans to develop NI2. NI2 could integrate automation to assist in information triage but is budgeted for completion in approximately two years. However, development of the automation to review SF-328s is not dependent on having NI2 in place, as the form is uploaded to the system and not completed in NISS today.

The FAST study team also learned about a current USG-funded effort by DARPA to create "TurboFCL," an online system that guides companies through completing complicated FCL forms and packages for submission. At the time of the FAST Study delivery, SF-328 guidance and examples are being integrated into TurboFCL, along with frequently asked questions about FOCI, structure for follow-up questions, and supplemental resources to assist companies in accurately completing initial submissions. By producing pre-structured data that companies can directly input into SF-328, TurboFCL will further assist in DCSA's ability to automate information triage. Pre-structured data provides consistency, which is essential for improving review quality and reducing rework, and critical for enabling responsible use of automation tools and AI for error checking, completeness validation, and pattern recognition across submission.

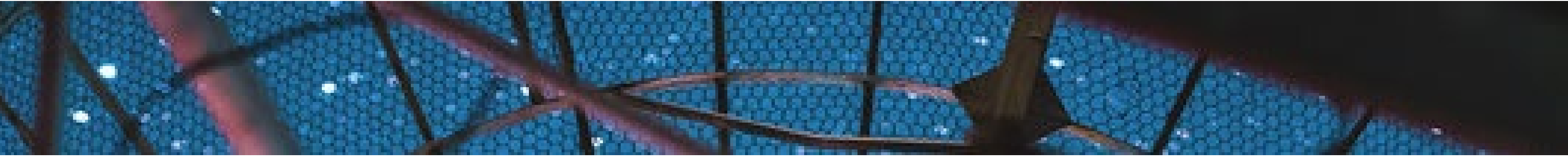
These tools should not replace adjudication but will significantly reduce cycle time and improve accuracy, as well as throughput of the FOCI review process by allowing analysts to focus on higher-risk cases rather than correcting avoidable issues. Automation would review initial submissions during the triage phase to alert companies to errors and missing information more rapidly, reducing costs and delays caused by manual reviews and back-and-forth communications between DCSA and companies. In turn, this will reduce DCSA review burden and allow industry to move through the FOCI portion of the Entity Clearance Eligibility process faster, ultimately enabling DOW projects to deliver to the warfighter earlier and at lower cost. Together, TurboFCL and automation in error checking and completeness validation should enable more efficient submission and review processes.

Additionally, DCSA should prioritize the continuous evaluation and improvement of their SF-328 review processes to ensure efficiency and effectiveness. By consistently tracking response times and addressing inefficiencies, DCSA can avoid repeating past challenges, identify areas that require clarity, and maintain a streamlined process. Continuous improvement is essential to meet evolving demands and risk and ensuring an effective and efficient process.

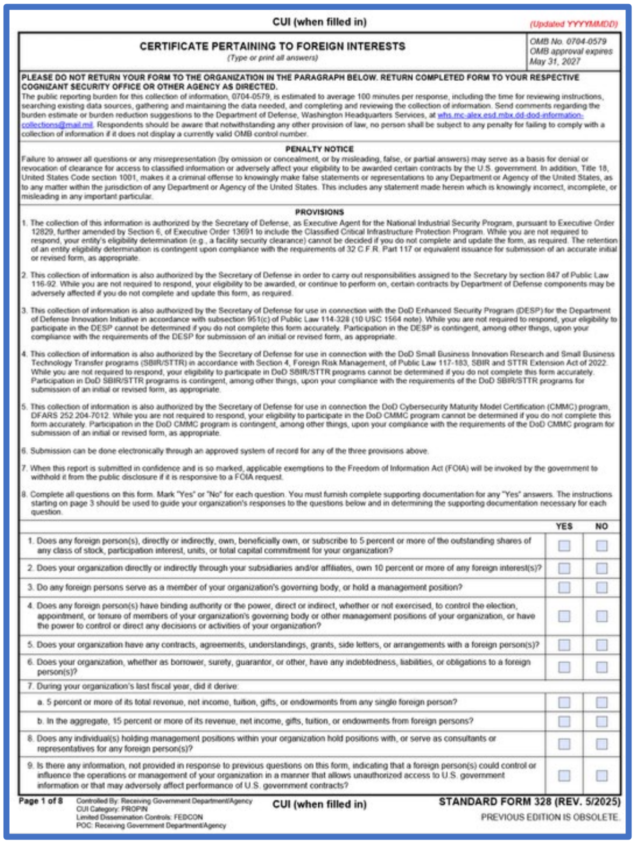
20) Understanding the New SF-328

Challenge

The new SF-328, approved May 2025, provides more detailed instructions and definitions than before, and reduces the number of questions by one. Figure 4, below, depicts the current SF-328. Interviewees appreciated these changes but noted the new form changes the existing questions to



be more granular and complex, necessitating additional costly legal and administrative review to ensure accuracy. Most interviewees (including existing defense contractors and new entrants) stated the new SF-328 requires additional time, resources, and new data collection (e.g., Questions 1, 2, 5-8). Based on interview and questionnaire responses, the estimated and/or actual labor hours to complete the new SF-328 ranges from 3 to 300 (average = 138 hours), depending on how many questions require a "yes" response and follow-up details. Interviewees described challenges translating SF-328 government terminology into common business terminology, creating difficulty for industry to identify the correct information needed and align it with the form. For example, interviewees described uncertainty about the level of detail and depth required in the organization chart and capitalization ("cap") tables. As one interviewee noted, "*we gave cap tables to the one percent, but still got asked for more*."



CUI (when filled in)

(Updated YYYYMMDD)

CERTIFICATE PERTAINING TO FOREIGN INTERESTS
(Type or print all answers)

OMB No. 0704-0579
OMB approval expires
May 31, 2027

PLEASE DO NOT RETURN YOUR FORM TO THE ORGANIZATION IN THE PARAGRAPH BELOW. RETURN COMPLETED FORM TO YOUR RESPECTIVE COGNIZANT SECURITY OFFICE OR OTHER AGENCY AS DIRECTED.

The public reporting burden for this collection of information, 0704-0579, is estimated to average 100 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding the burden estimate or burden reduction suggestions to the Department of Defense, Washington Headquarters Services, at whs.mc-alex.esd.mbx.dd-dod-information-collections@mail.mil. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

PENALTY NOTICE

Failure to answer all questions or any misrepresentation (by omission or concealment, or by misleading, false, or partial answers) may serve as a basis for denial or revocation of clearance for access to classified information or adversely affect your eligibility to be awarded certain contracts by the U.S. government. In addition, Title 18, United States Code section 1001, makes it a criminal offense to knowingly make false statements or representations to any Department or Agency of the United States, as to any matter within the jurisdiction of any Department or Agency of the United States. This includes any statement made herein which is knowingly incorrect, incomplete, or misleading in any important particular.

PROVISIONS

1. The collection of this information is authorized by the Secretary of Defense, as Executive Agent for the National Industrial Security Program, pursuant to Executive Order 12829, further amended by Section 6, of Executive Order 13691 to include the Classified Critical Infrastructure Protection Program. While you are not required to respond, your entity's eligibility determination (e.g., a facility security clearance) cannot be decided if you do not complete and update the form, as required. The retention of an entity eligibility determination is contingent upon compliance with the requirements of 32 C.F.R. Part 117 or equivalent issuance for submission of an accurate initial or revised form, as appropriate.
2. This collection of information is also authorized by the Secretary of Defense in order to carry out responsibilities assigned to the Secretary by section 847 of Public Law 116-92. While you are not required to respond, your eligibility to be awarded, or continue to perform on, certain contracts by Department of Defense components may be adversely affected if you do not complete and update this form, as required.
3. This collection of information is also authorized by the Secretary of Defense for use in connection with the DoD Enhanced Security Program (DESP) for the Department of Defense Innovation Initiative in accordance with subsection 951(c) of Public Law 114-328 (10 USC 1564 note). While you are not required to respond, your eligibility to participate in the DESP cannot be determined if you do not complete this form accurately. Participation in the DESP is contingent, among other things, upon your compliance with the requirements of the DESP for submission of an initial or revised form, as appropriate.
4. This collection of information is also authorized by the Secretary of Defense for use in connection with the DoD Small Business Innovation Research and Small Business Technology Transfer programs (SBIR/STTR) in accordance with Section 4, Foreign Risk Management, of Public Law 117-183, SBIR and STTR Extension Act of 2022. While you are not required to respond, your eligibility to participate in DoD SBIR/STTR programs cannot be determined if you do not complete this form accurately. Participation in DoD SBIR/STTR programs is contingent, among other things, upon your compliance with the requirements of the DoD SBIR/STTR programs for submission of an initial or revised form, as appropriate.
5. This collection of information is also authorized by the Secretary of Defense for use in connection the DoD Cybersecurity Maturity Model Certification (CMMC) program, DFARS 252.204-7012. While you are not required to respond, your eligibility to participate in the DoD CMMC program cannot be determined if you do not complete this form accurately. Participation in the DoD CMMC program is contingent, among other things, upon your compliance with the requirements of the DoD CMMC program for submission of an initial or revised form, as appropriate.
6. Submission can be done electronically through an approved system of record for any of the three provisions above.
7. When this report is submitted in confidence and is so marked, applicable exemptions to the Freedom of Information Act (FOIA) will be invoked by the government to withhold it from the public disclosure if it is responsive to a FOIA request.
8. Complete all questions on this form. Mark "Yes" or "No" for each question. You must furnish complete supporting documentation for any "Yes" answers. The instructions starting on page 3 should be used to guide your organization's responses to the questions below and in determining the supporting documentation necessary for each question.

	YES	NO
1. Does any foreign person(s), directly or indirectly, own, beneficially own, or subscribe to 5 percent or more of the outstanding shares of any class of stock, participation interest, units, or total capital commitment for your organization?	□	□
2. Does your organization directly or indirectly through your subsidiaries and/or affiliates, own 10 percent or more of any foreign interest(s)?	□	□
3. Do any foreign persons serve as a member of your organization's governing body, or hold a management position?	□	□
4. Does any foreign person(s) have binding authority or the power, direct or indirect, whether or not exercised, to control the election, appointment, or tenure of members of your organization's governing body or other management positions of your organization, or have the power to control or direct any decisions or activities of your organization?	□	□
5. Does your organization have any contracts, agreements, understandings, grants, side letters, or arrangements with a foreign person(s)?	□	□
6. Does your organization, whether as borrower, surety, guarantor, or other, have any indebtedness, liabilities, or obligations to a foreign person(s)?	□	□
7. During your organization's last fiscal year, did it derive:		
a. 5 percent or more of its total revenue, net income, tuition, gifts, or endowments from any single foreign person?	□	□
b. In the aggregate, 15 percent or more of its revenue, net income, gifts, tuition, or endowments from foreign persons?	□	□
8. Does any individual(s) holding management positions within your organization hold positions with, or serve as consultants or representatives for any foreign person(s)?	□	□
9. Is there any information, not provided in response to previous questions on this form, indicating that a foreign person(s) could control or influence the operations or management of your organization in a manner that allows unauthorized access to U.S. government information or that may adversely affect performance of U.S. government contracts?	□	□

Page 1 of 8

Controlled By: Receiving Government Department/Agency
CUI Category: PROPIN
Limited Dissemination Controls: FEDCON
POC: Receiving Government Department/Agency

CUI (when filled in)

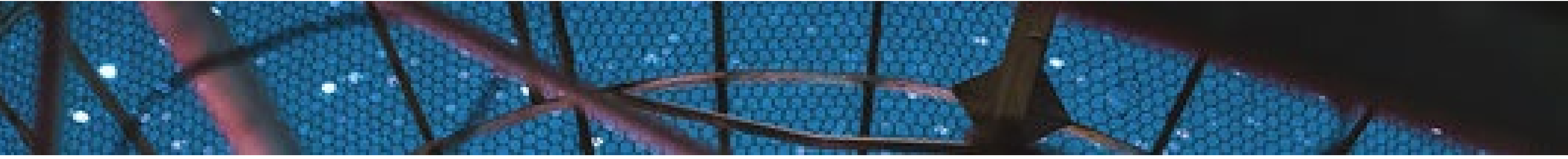
STANDARD FORM 328 (REV. 5/2025)
PREVIOUS EDITION IS OBSOLETE.

Figure 4. Updated SF-328

Common points of confusion included defining foreign beneficiaries and contracts, and how far down the supply chain and investor levels industry must document, especially as the information is challenging to obtain. The SF-328 requires proprietary or business sensitive information not typically shared, and interviewees described obtaining information from Venture Capital (VC) firms as particularly difficult. Companies commonly ask investors to speak with DCSA directly, further delaying SF-328 submission. As one interviewee elaborated, "*many ISRs [Industrial Security Representatives] lack training to assess modern ownership/VC model as it relates to FOCI, forcing delays, it's a struggle.*" Additionally, interviewees expressed difficulty in understanding what constitutes a material change within the supply chain, which remains unclear as described in the SF-328 instructions or by DCSA. For a large company with many foreign suppliers, changes in the supply chain are common and may not be deemed by the company as a material change. The Defense Security Service, since renamed DCSA, previously issued Industrial Security Letter (ISL) 2009-03[88] in 2009, to clarify reportable material changes. However, ISL 2009-03 was not updated and instead cancelled in 2021 as part of the NISPOM rewrite.[89] No replacement ISL has been issued, therefore, there has been no clarity or guidance for several years.

[88] Defense Security Service (2009). *ISL 2009-03.* Source: https://www.dcsa.mil/Portals/91/Documents/CTP/tools/ISL_2009_03.pdf

[89] DCSA (2025). *Voice of Industry.* Source: https://www.dcsa.mil/Portals/128/Documents/CTP/tools/251231%20VOI%20Newsletter.pdf



To add to the confusion, some companies have opted or been advised to use the outdated, cancelled ISL which remained accessible on the DCSA website at the time of the report.

Furthermore, interviewees varied in understanding the intent of more scrutiny into indirect ownership and lower-tiered (e.g., Tier 2 or Tier 3) investors and suppliers. They had mixed opinions about whether the deeper look required by the new SF-328 is collecting productive information and leveraging an effective risk-based approach. For example, several interviewees noted the new instructions in SF-328 Question 5 require information that appears more relevant to supply chain security than FOCI (e.g., capturing all suppliers of foreign-derived products or services rather than honing a risk-based approach), and details that may be classified (e.g., identity of USG customers).

Recommended Government Action

DCSA should continue to collaborate closely with industry to ensure SF-328 terminology is consistent with common business terminology, enabling industry to easily identify appropriate information to include in supplemental documentation. Industry needs additional DCSA guidance on the new SF-328, clarifying precisely what levels to document within supply chains and investments, and defining “material change” within those levels. Clarifying material changes through an ISL is necessary for DCSA to obtain appropriate reports from industry, which are essential to potential risk identification and maintaining a secure DIB.

Companies are becoming ever-more globally connected, especially among NDCs. The international ecosystem creates challenges for companies in providing appropriate information in the SF-328 and increases the complexity of information that DCSA must review. NDCs will be dissuaded from participating in the NISP if they perceive the SF-328 as too burdensome for their international business structure or are not confident in DCSA’s ability to understand and work with the nuances of their company’s organizational or funding structure. To facilitate NDC involvement in the NISP, DCSA must better account for nuances of VC, startups, and investment types and structures in its review. Based on FAST Study data, DCSA needs to provide DCSA staff with education and training on areas such as modern ownership models, VC models, diluted versus outstanding investments, investment structures, private equity structures, seed investors, and cap tables. To address industry’s challenges in obtaining information from investor companies, DCSA should establish a database of investor companies, including a trusted VC registry with periodic revalidation. This database should list VC companies and associated risks but *not* include details about the companies funded by them which is often deemed sensitive market information. This VC database will reduce the time burden on DCSA by eliminating frequent direct communication with VC companies. The *Modernizing the FOCI Approach* challenge provides additional recommendations on a specific FOCI study, including recommending analyses of new SF-328 instructions and measuring the form’s effectiveness in identifying FOCI risk.

FOCI-Mitigated Company Experience

FOCI-mitigated companies are a small but critical portion of the DIB, providing key innovation, technology, and support to the warfighter. Interviewees emphasized FOCI-mitigated companies undergo extensive additional review and approval processes, often earning higher DCSA security ratings due to their leadership's investment and commitment to supporting national security, the USG mission, and the warfighter. Although the presence of FOCI does not preclude companies from NISP participation, FOCI-mitigated companies must overcome barriers from negative perceptions and increased costs and delays. As one interviewee stated, "*DOW says that FOCI companies are not at a disadvantage, but this is not true, we have additional hurdles compared to non-FOCI companies.*"

21) Negative Perceptions of FOCI-Mitigated Companies

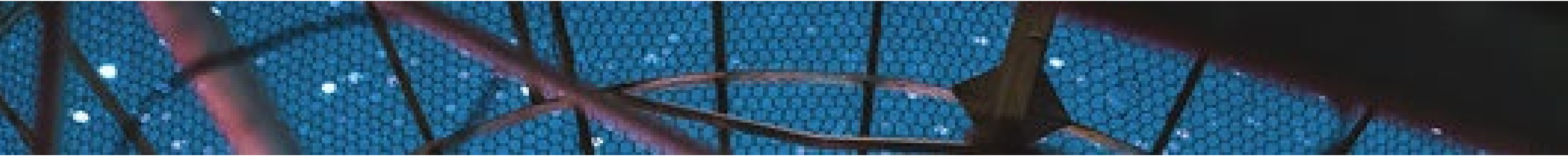
Challenge

Interviewees at FOCI-mitigated companies expressed significant challenges due to negative perceptions of their company's FOCI status. Examples included MILDEPs misunderstanding FOCI risk or the "FOCI-mitigated" terminology or being unwilling to wait for elongated processes due to FOCI mitigations. This negative perception makes it harder for FOCI-mitigated companies to start new work with the DOW as prime contractors or subcontractors.

> *"The perception of risk associated with our FOCI status often discourages both government customers and prime contractors from selecting our company, despite the mitigations in place. As such we must undergo additional scrutiny and risk exposure simply to participate in solicitations."* – Industry interviewee

During the FAST Study, the team learned that some DOW solicitations require companies to submit a SF-328 when submitting a proposal, even though it is not required by policy at that stage. The SF-328 submission at solicitation creates real challenges as some acquisition offices require companies to submit obsolete versions of the SF-328. Given the time and cost to complete the SF-328, companies working with multiple government customers must dedicate additional corporate overhead resources to complete different versions of the same form. In addition, when responding to solicitations as a subcontractor, prime contractors (offerors) frequently request access to the subcontractor's SF-328, which contains sensitive and proprietary business information (e.g., proprietary business relationships, financial arrangements, and strategic decisions not intended for public disclosure). Interviewees emphasized that sharing this level of information with a prime contractor prior to contract award creates financial, operational, and intellectual property risks.

More importantly, if perceived FOCI risk is considered in contract decisions, then requesting the SF-328 without simultaneously requesting information on approved mitigations immediately creates a disadvantage to FOCI-mitigated companies. Mitigations address, reduce, or negate FOCI risk, and FOCI-mitigated companies prioritize strong security postures. As one interviewee noted, "*we recognize the need to fight negative perception, which is why we have stronger programs.*" Consequently, mitigations must also be considered during contract decisions to ensure FOCI-mitigated companies are not disadvantaged simply due to their FOCI status. Lastly, interviewees noted contract documentation questionnaires and inquiries commonly include a "check box" question of whether the company is foreign-owned, without accompanying questions regarding



mitigation status. A simple “yes/no” question does not reflect an adequate understanding of mitigation requirements and disadvantages FOCI-mitigated companies if acquisition officials do not also consider DCSA’s review and mitigation approvals during the proposal phase. These challenges are rarely overtly discussed or acknowledged as reasons FOCI-mitigation companies are not selected for contracts; instead, FOCI-mitigated companies receive feedback such as “we decided to go in a different direction” since USG are not allowed to down select based on FOCI status.

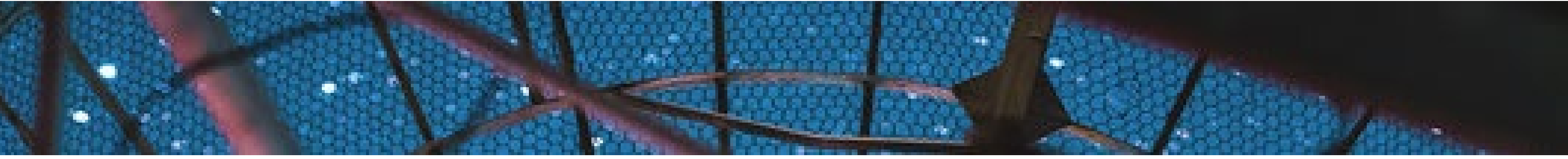
Recommended Government Action

OUSW(I&S) should issue a Directive-Type Memorandum (DTM) clarifying that the SF-328 is only ever sent directly to DCSA, prohibiting inclusion in solicitation documentation. DCSA, not acquisition officials, possess the responsibility and expertise to review the SF-328, identify FOCI concerns, and determine mitigation measures. Acquisition officials must not attempt to overstep DCSA’s authority by managing or pre-determining existing mitigations through solicitations. If questions about FOCI arise, acquisition officials should coordinate with DCSA FOCI experts directly, rather than with industry. Intentional coordination on all FOCI matters will negate the need for both prime contractors and subcontractors to share the SF-328 with acquisition officials.

If acquisition officials insist on asking about FOCI in solicitations or contract documents, they must move away from a “yes/no” question to prevent exclusion of FOCI-mitigated companies. Instead, companies could certify response options such as 1) no FOCI, 2) FOCI present and no approved mitigations in place, and 3) FOCI present and approved mitigations in place. The preferred question should be “is your company FOCI-mitigated and approved by DOW or other government agency, if yes explain.”

Acquisition officials should also consider the presence of approved mitigation plans when making award decisions rather than simply the presence or absence of FOCI, as well as ask for companies’ security ratings. Higher security ratings and approved mitigation plans are positive indicators of a strong security program. Additionally, source selection training should be updated to provide acquisition officials with a better understanding of FOCI and FOCI mitigations. DCSA should verify the accuracy of interviewees’ statements that FOCI-mitigated companies have higher security ratings; once confirmed, this information should be incorporated into trainings. See *Integration of Security into Acquisition Processes and Contracts* for further discussion on integrating security into acquisitions.

If DOW and OUSW(I&S) want to expand the DIB, they must reduce negative perceptions of FOCI-mitigated companies within USG. Education and outreach on mitigation instruments and security performance is urgently needed as USG prepares to implement Section 847, which will widen the pool of FOCI-mitigated companies. It is in the USG’s best interest to reduce negative perceptions, or risk losing many innovative and successful companies from the DIB. Acquisition decision-makers must understand that being FOCI-mitigated is not negative, and risk is actively managed through approved mitigations and oversight. USG must recognize that approved mitigation plans render FOCI companies as lower risk and should not result in opportunity loss. Perception management is critical to balance the potential cost of losing companies from the DIB.



22) Delays in Finalized FOCI Mitigation Agreements

Challenge

For a new FOCI company entering the NISP, interviewees described the process from submitting an Entity Clearance application to obtaining an Entity Clearance Eligibility taking up to three years. The process timeline is increased for FOCI companies, which typically have more complex and voluminous data to gather and document in the SF-328 for DCSA review. Additionally, if FOCI is present, DCSA FOCI Action Officers will coordinate FOCI mitigation requirements with companies. According to the FCL Orientation Handbook,[90] "a facility where FOCI is present will also take a longer time to clear because these facilities must undergo satisfactory FOCI mitigations." Although DCSA negotiates interim letters with FOCI-identified companies to begin work, companies must often wait several months to more than two years for DCSA to sign and finalize negotiated agreements. Interim security measures are often more stringent than negotiated agreements, which adds costs, delays delivery, and reduces the quality of the end product delivered to warfighters. In one example of the interim experience, a FOCI-mitigated company was unable to interact with their parent company to obtain commercial technology, which delayed availability and integration of warfighter capabilities from the parent company for over a year.

Recommended Government Action

DCSA should eliminate delays in finalizing negotiated agreements by requiring more rapid DCSA final signatures/approval processing. This will enable FOCI-mitigated companies to start DOW work faster and effectively leverage resources for security measures in line with final mitigations. See *Modernizing FOCI Approach* for further recommendations on increasing efficiencies in FOCI processes.

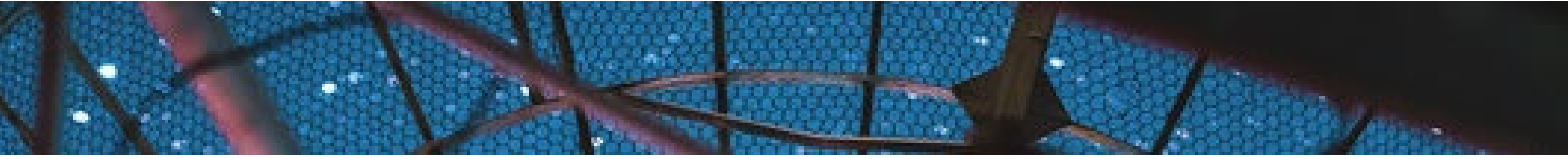
23) Ineffective Use of Outside Directors and Government Security Committees

Challenge

Interviewees shared challenges with the roles and responsibilities of Outside Directors (ODs) and other Government Security Committee (GSC) members. They emphasized that ODs and GSCs lack critical authorities, relying too heavily on DCSA's decision-making which reduces the implementation speed for FOCI risk mitigations. Interviewees appreciated the CDSE course offering in OD/PH training,[91] but expressed that the course is not widely known and some of the content is too high-level to be effective. Increased communication between ODs and DCSA is needed beyond the annual DCSA conference. Further, interviewees described that depending on FOCI type and associated mitigation plans, an OD can be hired in an advisory role rather than a voting board member. Although DCSA emphasizes the OD role's importance, this conflicts with

[90] Defense Security Service (2018). *FCL Orientation Handbook*. Source: https://www.dcsa.mil/Portals/128/Documents/CTP/FOCI/FCL_Orientation_Handbook_10OCT18.pdf?ver=cW4Mg1SLfHcAu8jM_gbNtw%3d%3d

[91] CDSE (n.d.). *Outside Director/Proxy Holder Baseline Training IS175.CU*. Source: https://www.cdse.edu/Training/Curricula/IS175/



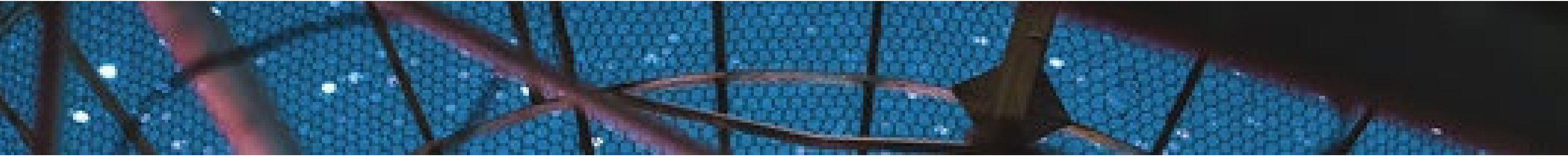
a company governance perspective when the role is outside of entity governance, creating a lack in clarity among leadership in what the OD can and cannot do.

> “*If we want to use something that a foreign parent can do that does not touch anything sensitive, we would have to go to DCSA for a request. Another company not under FOCI can use a foreign subsidiary without having to get permission.*” – Industry interviewee

Existing FOCI-mitigated companies reported experiencing delays due to DCSA reviews and approvals on items such as FOCI instruments, new or updated agreements, and updated supplemental policies. As one interviewee described, “*I’ve had supplements with DCSA for over a year and haven’t gotten feedback.*” Another interviewee stated it took their company 19 months for DCSA to finalize an updated proxy agreement that was largely unchanged and contained primarily administrative changes. The FAST Study identified that delays due to DCSA approval can take one to ten months. These delays disadvantage FOCI companies due to commercial opportunity losses, delays in starting work, and inability to leverage resources which their non-FOCI companies peers can access faster without approval. Interviewees at FOCI-mitigated companies noted collaboration with international subsidiaries requires extensive reviews, technology control measures, and authorizations that delay or prohibit sharing of otherwise releasable information. This control hinders the ability of FOCI-mitigated companies to integrate capabilities and specialized foreign expertise that optimizes operations and enhances the innovative products delivered to the warfighter. Interviewees noted additional examples of activities requiring lengthy DCSA approval processes:

- Linking websites to a parent organization website
- Specifying named individuals in shared services and reverse shared services
- Comarketing events
- Leveraging parents’ sales and marketing teams for inbound leads
- Selection of third-party shared service providers

Lastly, default mitigation documentation, such as the Affiliated Operations Plan (AOP) often formally require DCSA approval for a variety of changes, such as changes in operations, AOP terms, security protocols, personnel, and affiliated entities. Interviewees described that as a FOCI-mitigated company matures and demonstrates success, the AOP is often renegotiated and adjusted based on risk to provide a company with more internal decision-making authority; in those instances, the company would be able to notify DCSA of changes that previously required DCSA advance approval. Upon notification, DCSA can engage the company to either clarify or disagree with the change. However, interviewees identified several areas within mitigation documents (e.g., AOP) where both DCSA and industry would benefit from leveraging the authority of the OD and GSC to make decisions from the time of AOP approval rather than being renegotiated over time.



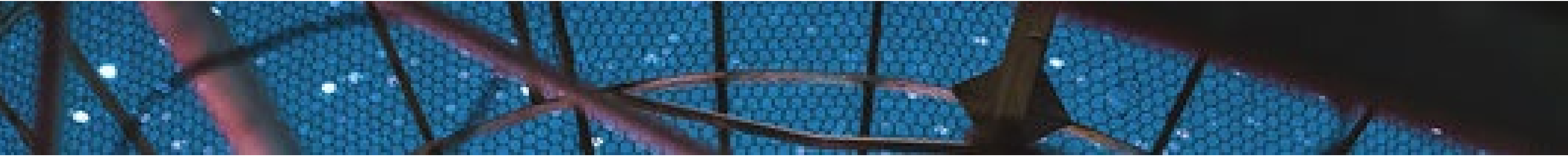
Recommended Government Action

DCSA should process administrative changes faster. Interviewees recommended leveraging regional directors to process administrative changes quickly, allowing ISRs to focus on more complex changes. DCSA should also integrate business terminology into mitigation documentation and OD/PH training so companies can more quickly and accurately understand mitigation implementation and business impacts. Further, the OD role must be clarified so companies can understand whether the role is on the board, an advisor, a special advisor, or a board observer. If precise language is not used, boards may reject a potential FOCI mitigation because the OD role is not elevated leading the board to deem DOW work, as some interviewees put it, to not be "worth it." When ODs are not required to be board members, DCSA should encourage companies to ensure the ODs have the authority that both complies with company governance and empowers ODs to protect national security through entity governance. Lastly, DCSA should conduct more regional and individual meetings with ODs to facilitate direct engagement. Such meetings create opportunities for DCSA to discuss company-relevant risks, and how ODs and DCSA can collaborate to monitor and address those risks. In addition, the meetings would augment information available to DCSA to better support decision-making and understand what risks should be given weight at a particular company.

ODs and GSCs are expensive and should be better leveraged to make more decisions without DCSA approval wherever appropriate. FOCI-mitigated companies are motivated to support national security, and pay significant amounts of money to hire legally liable ODs. Many ODs are near the end of or have recently completed distinguished careers in national security-related fields. DCSA should expand their partnership with ODs by relying on them to exercise discretion in a wider range of decisions and encourage more frequent exchange of information and better ways to leverage their role in the company. For example, DCSA can use a Service Level Agreement (SLA) model for approvals, with pre-approved categories of low-risk operational changes, and periodic joint reviews with documented rationales. Qualifications for the OD role are defined in policy, leaving DCSA latitude to decide responsibilities during implementation. DCSA should identify areas for immediate change in authorities such as normal business processing and more flexible visitor policies. Notably, leveraging ODs and GSCs more does not counter requirements for DCSA oversight, as their decisions must still be reported to DCSA. Ultimately, relying more on ODs and GSCs will save DCSA time and reduce the burden of extensive reviews and approvals among FOCI-mitigated companies while maintaining DCSA oversight.

As FOCI-mitigated companies mature and demonstrate successful security processes, DCSA should continue to adjust documentation to provide companies with more internal decision-making authority. However, interviewees identified decisions where notification as opposed to approval from DCSA should be implemented now as the baseline, rather than being expanded over time. These decisions involved:

- **Shared third parties:** Shared third parties include providers of services (e.g., auditors, lawyers, investment bankers) that are shared between an entity and its affiliate. Interviewees emphasized that the GSC exists to oversee auditor selection, and that it should be a company



decision without DCSA’s involvement. Default language should relinquish the requirement for prior approval from DCSA for audit firm changes.

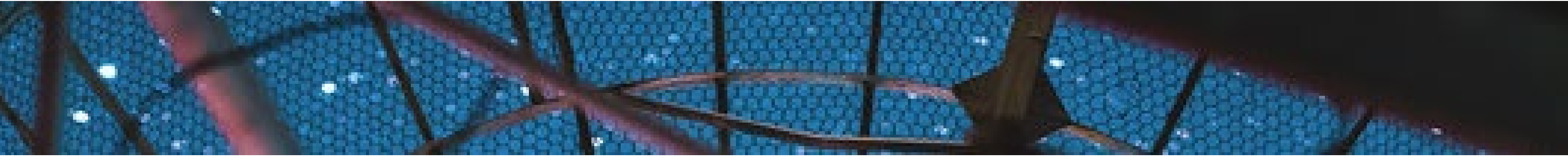
- **Shared employees:** Interviewees noted that shared employees (i.e., affiliate company employees assigned to work with the company or vice versa) must be individually named. Given the lengthy process to obtain DCSA approval on changes, specific employees may change or leave the company while awaiting approval. DCSA should consider identifying categories of employees, rather than specific individual names.
- **Cooperative commercial arrangements**: Cooperative commercial arrangements are commercial agreements with affiliates to collaborate while maintaining independence, and can range across many categories of services (e.g., human resources, finance, internal audits, business development). Interviewees recommended leveraging risk-based tiers to expedite the approval process for cooperative commercial arrangements. At the lowest tier, internal company management may approve the decision and notify DCSA. At the highest tier (e.g., involving classified work), DCSA approval may be required on an expedited basis.

Entities with limited FOCI (referred to as “FOCI light”) rely on a Special Board Resolution (SBR) or Board Resolution (BR), which clarifies when the board and senior management officials can make certain decisions. Interviewees anticipate SBR to be the most prevalent mitigation type in 2026 and emphasized the importance of enabling more rapid board level decision-making through notifications rather than approvals from DCSA. Doing so will release key DCSA resources to address more complex issues with “FOCI heavy” companies.

See *Current FOCI Approach is Outdated* for recommendations on FOCI study areas, including evaluating the roles, responsibilities, and qualifications of ODs and GSCs.

Supplemental FOCI Documentation and Templates

FOCI forms are complex, and already require supplementary documentation. In addition to the SF-328 itself, FOCI-mitigated companies must prepare and maintain instruments such as Electronic Communications Plans (ECPs), Affiliated Operations Plans (AOPs), and Technology Control Plans (TCPs), many of which come with associated DCSA templates and guides. Interviewees emphasized that these supplemental artifacts are often highly granular, not written in plain-English business terminology, and require extensive coordination across company leadership, affiliates, general counsel, and external legal consultants. In some cases, the supplementary guidance itself even requires *its own* supplementary guidance. This complexity creates a barrier to entry, particularly for NDCs and small and medium-sized businesses; many of these companies must rely on Security-as-a-Service providers or specialized legal counsel to interpret and complete the required supplementary documentation, adding significant cost and delay. Larger companies already established in the DIB are better able to absorb these expenses as part of their corporate overhead, but for smaller businesses or new entrants, the same costs can be prohibitive, discouraging participation and limiting the pool of innovative firms willing and able to become FOCI-mitigated and support the DOW mission.



24) Need for Modernized Electronic Communications Plans

Challenge

Several interviewees questioned the efficacy of ECPs in their current format. ECPs require monitoring and filtering of email communications from parent companies, despite security controls already preventing FOCI-mitigated companies from emailing sensitive information (e.g., export control requirements, classified information protections). Consequently, FOCI-mitigated companies expend time and technology budgets on redundant controls. In some cases, interviewees described that the ECP forced or constrained them to migrate to Microsoft solutions to enable monitoring capabilities. However, Microsoft is often more costly than other providers such as Slack, which interviewees described as the predominant provider across companies.

> *"FOCI mitigation instruments are decades old, a lot of focus on things that do very little to improve security but are burdensome." – Industry interviewee*

Recommended Government Action

DCSA should focus technology protections on technology transfer and anti-tampering monitoring to gain more confidence from DOW customers in FOCI-mitigated companies. Allow FOCI-mitigated companies to leverage resources for more modern technical capabilities such as Data Loss Prevention (DLP) solutions to monitor for technology transfer. DCSA can enact this change through a Memo to ISRs, followed by an ISL to industry and updated ECP template.

25) Burdensome Affiliated Operations Plan

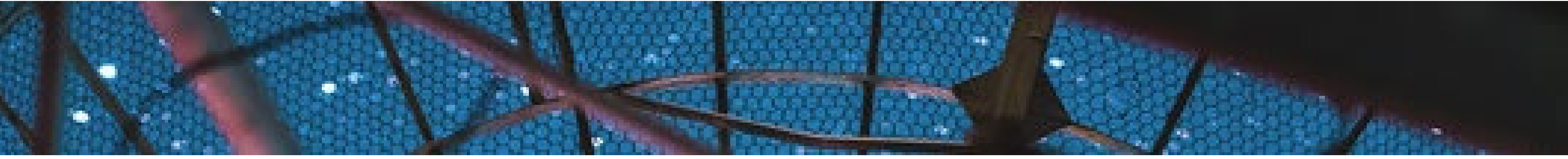
Challenge

AOPs typically take a company six months to create and finalize, and require coordination with company leadership, affiliates, general counsel, and legal consultants. Interviewees recognized AOPs as critical and requiring time to complete accurately. However, they also described a strong need to streamline AOPs. Specifically, AOPs identify program-level categories for shared services, with each category containing specific measures at a very granular detail. Security measures are often applicable across program categories, resulting in costly and time-consuming duplicative effort as industry manually completes the lengthy document.

Recommended Government Action

DCSA should build a "playbook" or collection of mitigations, governance techniques, and controls for various shared services based on risk. Once built, DCSA should share this playbook with companies requiring an AOP. The AOP playbook should be presented as baseline patterns with deviation paths, supporting the notion that security and acquisition are risk-based.

By adopting an AOP playbook, DCSA can more rapidly review and approve AOPs as industry would be able to use pre-approved terminology and approaches dependent on the specific circumstances of the FOCI-identified company. Similarly, this increased transparency would enable industry to more quickly propose and update approaches to DCSA.



Ultimately, the USG and industry will benefit as relevant risk-based approaches can be approved and implemented earlier than would be possible through current duplicative and time-consuming manual back-and-forth review and approval efforts. Over time, DCSA could integrate the AOP into NISS/NI2. Through future automation, DCSA could develop a NISS/NI2 capability to identify relevant areas of risk based on information a company provides and prepopulate the AOP with information on mitigation options that could be integrated.

DCSA should promote baseline mitigations to reduce the already-granular AOP's overall content. This would involve consolidating repetitive mitigation measures found across multiple program-level categories into a baseline mitigation section referencing the applicable categories; each program section would then describe the specific relevant technology. Additionally, DCSA should use a tiered structure to identify security measures based on risk, empowering companies to manage operational aspects under GSC oversight and approval on low-risk tiers (see *Ineffective Use of Outside Directors and Government Security Committees* for recommendations on leveraging the authority of ODs and GSCs). This will allow the GSC to manage in conjunction with DCSA, without the need to approve all changes to specific products and technologies. This action could save DCSA time reviewing AOPs or mitigations for lower risks, in turn reducing delays experienced by industry waiting for reviews to be completed. DCSA can also leverage risk tiering to identify what requests and updates must be reviewed and approved faster. Lastly, DCSA could institute transition periods for lower-risk or highly time sensitive issues, allowing companies to move forward after identifying risks, mitigations, and interim implementation measures pending proposed mitigation approval.

26) Outdated Templates and Guides

Challenge

Interviewees consistently described DCSA's templates and guides as helpful but limited in quantity and rarely updated. Interviewees highlighted the sample Technology Control Plan (TCP) template,[92] stating the document was created in 2012 and not accompanied by guidance. Similarly, the AOP Guide[93] was deemed helpful but outdated (11 May 2016). Both documents do not account for business and technology environment changes in the past decade. Lastly, interviewees noted the complexity of the ECP template,[94] which is not accompanied by a guidebook to clarify the detailed form.

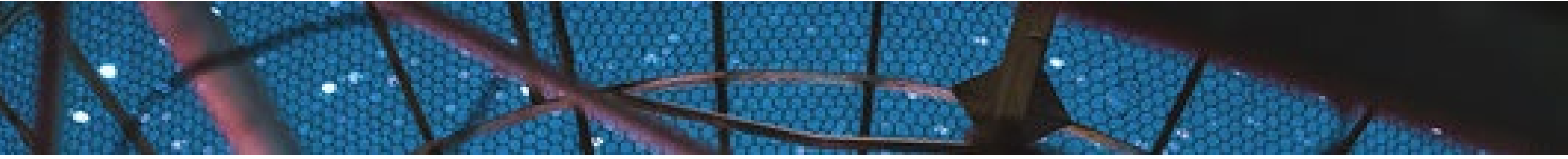
Recommended Government Action

DCSA should update the TCP template and AOP guide, in addition to producing guidance for the TCP and ECP. In developing templates and guidance, DCSA should continue to collaborate with industry as they did with the DCSA Authorization and Assessment Guide (DAAG) to identify

[92] DCSA (n.d.). *Sample Technology Control Plan.* Source: https://www.dcsa.mil/Portals/128/Documents/CTP/FOCI/TCP%20Sample%20230525.docx

[93] DCSA (n.d.). *Navigating the Affiliated Operations Plan.* Source: https://www.dcsa.mil/portals/128/documents/ctp/foci/AOP_Guide_51116.pdf

[94] DCSA (n.d.). *Electronic Communications Plan Template.* Source: https://www.dcsa.mil/Portals/128/Documents/CTP/FOCI/ECP%20Template%2020240325.docx



specific points of confusion, recommended changes, and language consistent with business terminology.

27) Duplication Between ECP and CMMC

Challenge

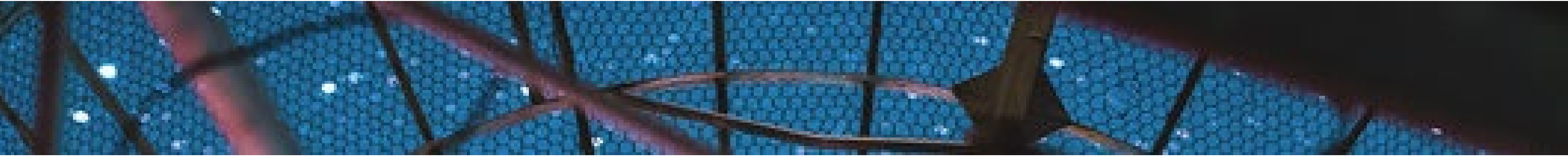
Most FOCI-mitigated interviewees described duplication between cybersecurity requirements for contractor unclassified information systems (CMMC Level 2/National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171) and classified information systems (32 CFR 117 and DCSA). ECP and CMMC require extensive industry and government time, including completing and reviewing documentation, and conducting and responding to assessments/audits. Companies said the documentation and USG review across elements within CMMC Level 2 and ECP are completely duplicative. Consequently, there is significant duplicated cost and effort which industry could better place on other operational and strategic security efforts. FOCI-identified companies end up receiving duplicate costs that are not incurred by companies without FOCI, placing them at a financial disadvantage.

Recommended Government Action

Since CMMC and ECP frameworks are derived from NISP SP 800-53 cybersecurity control families, interviewees recommend reusing validated CMMC artifacts for ECP's overlapping cyber controls. Specifically, interviewees ask that DCSA accept CMMC Level 2 certifications for ECP requirements. This change would enable DCSA to reduce the ECP in scope to only specific areas not already covered by CMMC (e.g., electronic communications monitoring). The FOCI mitigation instrument focused on those specific areas, referred to as an Electronic Communications Monitoring Policy (ECMP), should be the only documentation required for FOCI-mitigated companies with CMMC Level 2 to meet their ECP requirements. Accepting CMMC Level 2 evidence for the overlapping controls would be a risk-informed and efficient reuse of validated artifacts, not a relaxation of NISP requirements, thus reducing duplicative audits, documentation, and review time for both industry and DCSA and allowing DCSA to focus on higher-risk areas. Oversight of the ECMP approach can be maintained through structured sampling, targeted checks, and unannounced "snap" review of CMMC evidence.

NDAA Section 847

Section 847 of the FY20 NDAA is a significant step enhancing DOW's ability to identify and mitigate FOCI risks in unclassified contracts and subcontracts. In expanding current FOCI vetting requirements to pre-award and unclassified contracts, Section 847 represents one of the largest defense acquisition security reforms in recent decades. As the world becomes interconnected in new ways, and adversaries try to take advantage, it is critical for companies with foreign ties to maintain security measures protecting the USG-funded innovation and technology delivered to the warfighter.



28) NDAA Section 847 $5M Threshold Remains Undefined

Challenge

Under Section 847, covered contractors or subcontractors include existing and prospective contractors and subcontractors of the DOW on contracts, subcontracts, and/or defense research assistance awards exceeding $5M. Almost all interviewees expressed concern regarding how the $5M threshold will be defined and implemented, and emphasized the need for clear guidance. Based on FAST subject-matter expertise, depending on how the $5M threshold is defined and implemented, it may impact security, cost, schedule, and performance:

- **Security:** Immediate FOCI determination and mitigation could be required for existing work; government could potentially issue a stop-work order.
- **Cost:** Compliance, legal, and governance costs might be incurred if not properly addressed during the proposal phase; potential idle or loss of labor or clearances during a pause.
- **Schedule:** The ability to exercise option terms or permit services to commence under the option period may be delayed. In an existing Indefinite Delivery Indefinite Quantity (IDIQ) situation, the selection of an order awardee (if the order is competed amongst IDIQ multiple award contract holders) could be prolonged thus defeating the purpose of using an IDIQ as a streamlined vehicle to order services. Either scenario could lead to program or contract milestone slippage or resequencing while the FOCI determination/mitigation is completed.
- **Performance:** Reduced efficiency and schedule impacts as described above ultimately impact delivery to the warfighter. If teams or facilities are restricted, necessitating performance at alternate cleared locations or with different personnel, there will be risk to quality and timeliness until mitigations are in place.

Recommended Government Action

OUSW(A&S) must clearly describe now how “exceeding $5M” will be defined and implemented. This is imperative for offerors and existing contractors to understand and comply with the requirements, as well as include the related costs in their proposals submitted in response to solicitations and potential FOCI-related contract modifications. Based on interviewee feedback, threshold considerations include contracts at $5M guaranteed with options, and IDIQs where orders could add up to $5M. Given the volume of contracts and subcontracts over the $5M threshold, interviewees recommend that OUSW(A&S) consider technology type when determining the $5M threshold to balance contractual award amount against criticality and vulnerability without overwhelming the FOCI system. Some interviewees recommended leveraging the Industrial Base Technology List (IBTL), which was previously used during comprehensive security reviews because it is unclassified and accessible to industry. In Table 6, FAST Study SMEs identified potential interpretations for defining the $5M threshold under various contract vehicles.

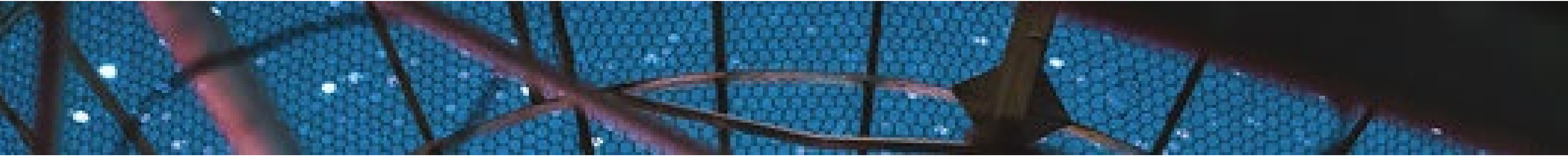
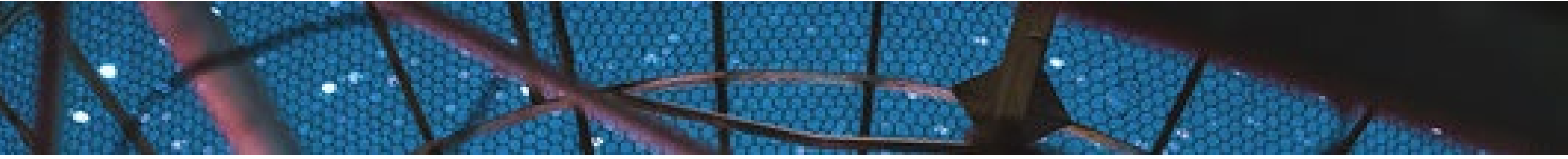


Table 6. Example Interpretations of the NDAA 2020 Section 847 $5M Threshold

Contract Vehicle	Options for Defining $5M Threshold
IDIQ	- The minimum quantity set forth in the IDIQ solicitation results in the offerors' awarded dollar value* for that minimum IDIQ quantity exceeding $5M. - The minimum quantity set forth in the IDIQ award did not result in the offerors' dollar value* for the minimum IDIQ quantity exceeding $5M, but subsequent orders* do exceed $5M. Subsequent orders are considered as exceeding $5M when the first task order award* exceeds $5M or when a task order award* will cause the aggregated total dollar value of awarded* task orders to first exceed $5M. - The minimum dollar value set forth in the IDIQ solicitation* exceeds $5M. - The minimum dollar value set forth in the IDIQ award* did not exceed $5M, but subsequent orders* do exceed $5M. Subsequent orders are considered as exceeding $5M when the first task order award* exceeds $5M or when a task order award* will cause the aggregated total dollar value of task order awards* to exceed $5M. *Applies to the total value of the base period (inclusive of optional quantities) and all option periods (inclusive of optional quantities).
Contract (non-IDIQ)	- Contract value is deemed as exceeding $5M when a contract is awarded at a total dollar value exceeding $5M, including the base period and all option periods (inclusive of optional quantities).
OTAs	- Not all OTAs require a dollar ceiling and may include unpriced CLINs. An OTA may be awarded with an expected value that would not exceed $5M. However, the OTA's inherent flexibility could ultimately allow for additional services that increase the dollar value to exceed $5M, thereby triggering compliance with Section 847.
Orders Against a GSA Master Services Agreement (MSA) Awarded by Non-DOW Agencies	- Since GSA MSAs are awarded by GSA, they typically do not include DOW requirements at the MSA level. However, orders issued against these MSAs can incorporate agency-specific clauses as needed. It is important to note that using an MSA vehicle (awarded by a non-DOW agency/component) does not exempt DOW from adhering to their own regulations and policies, such as those for FOCI. - Therefore, when the Section 847 requirement comes to fruition, it would apply to an order issued against the GSA MSA. A DOW order against a GSA-MSA would likely not be the only order placed against that GSA-MSA contract. Other DOW orders may be issued by that same program or other MILDEPs, thus increasing the likelihood that the $5M could rapidly be exceeded for the contractor, if not exceeded when the first order is placed. While GSA contracts include commercial products and services, some may not. Additionally, according to the above covered contractor or subcontractor definition, even commercial products or services that are excluded, could be subject to the FOCI requirements if the designated Principal Staff



	Assistant (PSA) or MILDEP official determines that the contract involves a risk or potential risk to national security or potential compromise of sensitive data, systems, or processes such as personally identifiable information, cybersecurity, or national security system. • When services or products are anticipated to be those that would be provided by a covered contractor or subcontractor, issue a sources sought notice or RFI to assess the GSA MSA contract holder’s level of interest in submitting a proposal. This will help predict the level of interest/capability from covered contractors (or their anticipated covered subcontractors). This will help the government assess the potential for “competition” from GSA MSA holders if procuring non-commercial items/services or commercial items/services that the designated PSA or MILDEP official determines would involve a risk or potential risk to national security or potential compromise of sensitive data, systems, or processes such as personally identifiable information, cybersecurity, or national security system.
Orders Against Best-in-Class (BICs) and other GWACs (Awarded by Non-DOW Agencies) or Federal Supply Schedule	• The same concepts and considerations for MSA apply.

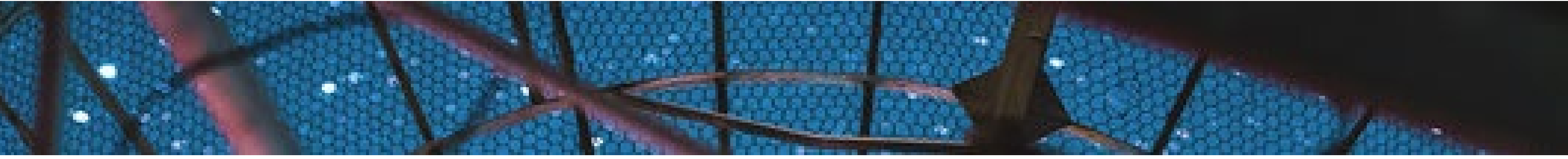
29) NDAA Section 847 Implementation Guidance Woefully Needed

Challenge

Interviewees recognized the importance of Section 847, examining supply chains, and properly vetting for FOCI risk. However, common points of frustration and concern were identified across interviewees. The primary concern is that 847 will “overwhelm the system,” resulting in slowed or stopped processes and limited availability among DCSA Industrial Security Representatives (ISRs).

> *“DCSA will be quickly overwhelmed with FOCI considerations for uncleared companies, and support/services/responses to cleared companies will suffer. I anticipate duplication of efforts and multiple simultaneous reviews of a company at the award level unless there is a repository of verified companies available for use by prime contractors when building teams.”*
> – Industry interviewee

Interviewees expressed uncertainty about when 847 will be implemented and are concerned that companies, particularly those not already in the NISP, will not have enough notice to prepare. Several interviewees fear companies, vendors, or suppliers already working with DOW on unclassified work will walk away if mitigations are perceived as too burdensome. Interviewees expressed frustration that companies with existing Entity Clearance Eligibility must also undergo a duplicative FOCI review for Section 847. As one interviewee described, “*it makes no sense to make companies in the NISP go through a Section 847 review. If we are cleared to have access to classified information, we should be all set to bid on anything.”*



Several aspects of Section 847 implementation will require additional guidance and clarification from the USG; however, five years have passed and industry has seen little to no progress on implementation guidance and how the $5M threshold will be defined. Currently, interviewees fear 847 will "*grind acquisition to a halt*." Industry critically needs guidance now to prepare for Section 847. As USG prepares additional documentation, interview feedback focused on recommendations for implementation.

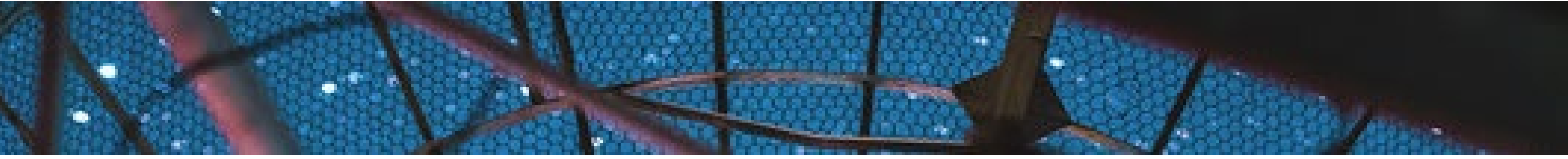
Recommended Government Action

Significantly Increase Awareness. Interviewees described that many companies outside the NISP do not know 847 is coming or what the SF-328 entails. Consequently, education and awareness efforts from OUSW(I&S) in coordination with OUSW(A&S) are needed to better prepare industry. A&S should consider adding a notice to solicitations and notifying contractors with contracts over the $5M threshold that once Section 847 is implemented, compliance will be required pre-award or post-award as applicable. This will provide increased awareness across industry, enabling industry to begin preparing for Section 847 implementation earlier. Additionally, DCSA should expand the Section 847 webpage[95] to provide additional guidance and resources to industry. Industry would benefit from a FAQ page, and examples of various cases to explain when and why Section 847 does and does not apply. When developing these resources, DCSA should solicit input from industry to identify common points of misunderstanding and language to ensure consistency between government and industry terminology.

Considerations for Existing Companies with Entity Clearance Eligibility. DCSA should consider cleared entities and existing FOCI-mitigated companies with an Entity Clearance Eligibility in good standing as already qualified under Section 847. These entities have already undergone FOCI review and have mitigations in place if necessary. Additionally, entities with an Entity Clearance Eligibility complete annual security reviews with DCSA and must already report material changes to the SF-328. These entities should continue to attest that nothing has changed, and that they will protect unclassified and Controlled Unclassified Information (CUI). Consequently, existing entities will still be checked but will not undergo a re-review. Considering these entities as already qualified leverages the principle of reciprocity and reduces duplicative efforts within both industry and government. Given Section 847's focus on unclassified contracting activity, non-cleared entities must be the primary focus rather than entities already handling classified information and under continual review. Additionally, DCSA should include information on existing mitigations when evaluating 847 and providing information to acquisition officials. This is important to prevent disadvantages to FOCI-mitigated companies and clarify that mitigations render FOCI risk low.

DCSA Availability. To address concerns about DCSA availability to companies in the NISP, DCSA should develop structured 847 reviews of the SF-328 to enable regional and field officers to review the form and ascertain when there is no need for further FOCI review or mitigation. This empowers regional and field officers and frees headquarter-level resources to work directly with FOCI-mitigated companies.

[95] DCSA (n.d.). *National Defense Authorization Act, Section 847.* Source: https://www.dcsa.mil/Section847/



FOCI Training and Awareness Among Acquisition Officials. According to procedures documented in DODI 5205.87,[96] DCSA will review covered contractors' FOCI documentation and produce a risk indicator report for KOs' use in source selection decisions. Given interview feedback on the negative perceptions of FOCI-mitigated companies, acquisition officials must have a sufficient understanding of FOCI and FOCI risks to prevent the exclusion of FOCI companies based on negative assumptions that may not be accurate. Acquisition officials must be risk-informed rather than risk-averse, and security professionals (e.g., acquisition security professionals) must be part of acquisition decisions to review and provide expertise on security and risk. Lastly, OUSW(A&S) implementation guidance must include that the SF-328 should be submitted directly to DCSA (and not directly to the KO).

Other Key Areas to Clarify. Interviewees raised additional questions surrounding Section 847 implementation that must be clarified in implementation guidance issued by OUSW(I&S) and OUSW(A&S). Interviewees highlighted that prime contractors and subcontractors need guidance on how to handle subcontracts, and how to verify that another partner company meets 847 requirements in order to predict teaming agreements. For companies already in the NISP, implementation guidance must clarify how the 847 determination affects existing Entity Clearance Eligibility and FCLs. Industry needs to understand differences between 847 and NISP (FCL) requirements, including the definition of change conditions, documentation, and updates or reporting. Additionally, the timing and process of flowing 847 requirements and documentation between acquisition offices, industry, and DCSA must be streamlined and clarified to address concerns that companies could miss opportunities resulting from either lengthy 847 reviews, or reviews triggered while on contract (such as during an IDIQ). Lastly, guidance must clarify processes for cases when a contract *might* exceed the $5M threshold at the time of award. In this case, an interviewee recommended granting the procuring agency authority to determine whether 847 reviews are necessary, depending on the sensitivity of the contract.

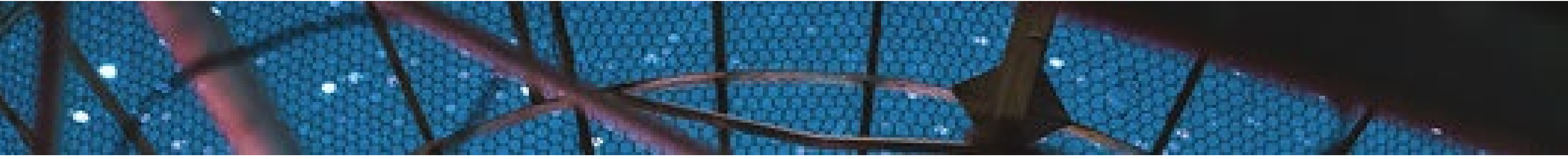
Modernizing FOCI Approach

30) Current FOCI Approach is Outdated

Challenge

Based on FAST study interview data, industry is clearly questioning the utility of the more in-depth level of information required by the new SF-328. Industry expressed concerns about the time and cost for industry to document the newly required and more detailed information, coupled with DCSA's time and cost to review. A majority of interviewees also expressed uncertainty on whether the new SF-328 captures the "right kind" of beneficial ownership and noted there should be a higher threshold for limited partners of entities without financial or ownership interest and governance rights. Interviewees did not view this type of limited partner as a FOCI risk given its inherent exclusion from the company, which is the basis of many mitigation resolutions. For example, an interviewee noted concern that the SF-328 goes too deep into the layers of beneficial ownership of fund-limited partnership interests by passive financial investors in private equity deals. Interviewees recommended excluding descriptions of the ownership structure of entities that

[96] DOD (2024). *DOD Instruction 5205.87: Mitigating Risks Related to Foreign Ownership, Control, or Influence for Covered DOD Contractors and Subcontractors*. Source: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/520587p.pdf



hold a beneficial interest in the filing entity solely through ownership of passive interests in an entity that itself holds only a passive interest in the filing entity.

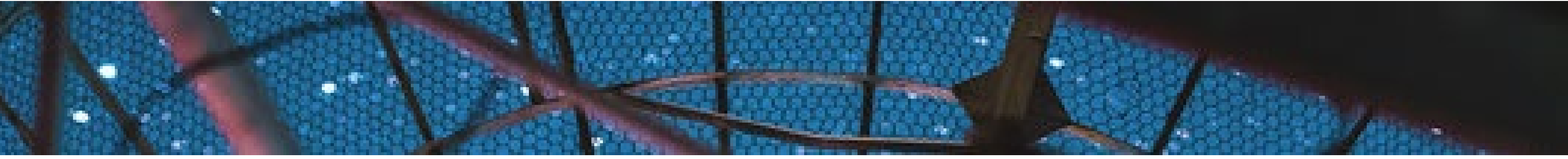
Given DOW's focus on modernizing defense acquisitions, now is a critical time to pause and evaluate whether the current FOCI approach is sufficiently risk-based and effectively mitigating risks in the least burdensome manner to industry. Interviewees described varying levels of complexity and challenges during the FOCI review process depending on FOCI status, type of FOCI, and other company nuances. Among FOCI-identified companies, the process was viewed as particularly challenging.

> "*Working through the FOCI process is very cumbersome, difficult, and often a one-sided conversation. This is made more challenging by not having a single point of contact to work through the process; there are so many units within the DCSA FCL branch, but no singular case officer to contact. It is like going to the DMV to update a registration, get a license, and a REAL ID; you have to go to three different windows and talk to three different representatives and none of them talk to each other*." – Industry interviewee

To date, no detailed, comprehensive analysis has leveraged DCSA's collected data to examine the effectiveness and proportionality of the full range of FOCI mitigation options. Although DCSA gathers substantial data, it is generally applied to day-to-day operational challenges and planning rather than overall program-level impact assessments.

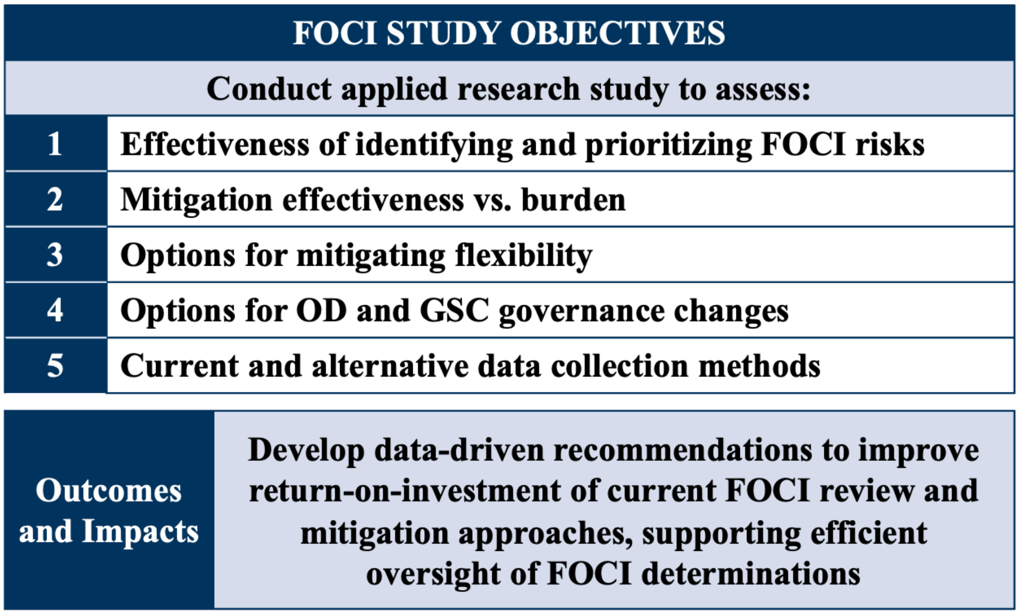
Company Experience: A FOCI-identified company has a longstanding relationship with IC customers, with existing IC-sponsored Entity Eligibility and classified facilities. The company is currently undergoing DOW Entity Eligibility Determination and FOCI with DCSA: the company was multiple times with a year passing between each submission and denial notification. After most recent submission, months passed before the company received any response from DCSA. The interviewee described the impact of these delays:

- *Opportunity Loss*: Backlog of DOW customers that want to issue classified contracts but cannot deliver a DD-254 without a DOW Entity Clearance.
- *Risk*: Interim solutions to receive DOW contracts included joint use of existing IC-accredited facility and receiving PCLs through IC sponsors and issuing clearance reciprocity, potentially creating need-to-know issues with risk absorbed by both customers and companies.
- *Administrative Burden to Government*: Approximately 25 staff received PCLs through the company's IC sponsors in order to start work. In most cases, the PCLs were processed as initial investigations and required polygraphs, which increased delays and administrative burden that would be otherwise unnecessary as DOW does not have a polygraph requirement.



Recommended Government Action

As oversight authority, OUSW(I&S) should fund a comprehensive study to evaluate DCSA’s current approach to FOCI, with a focus on quantitatively determining the return-on-investment of the current FOCI review and mitigation approaches, and potential data-driven modifications to the process. The proposed FOCI study would provide data-driven insights to increase DOW efficiency, decrease redundancy across CSAs, and ultimately streamline processes for industry to deliver to the warfighter faster. The proposed study would form a baseline for less cumbersome future OUSW(I&S) oversight of FOCI determinations. The proposed study should focus on the following objectives, as summarized in Figure 5.



FOCI STUDY OBJECTIVES	
Conduct applied research study to assess:	
1	Effectiveness of identifying and prioritizing FOCI risks
2	Mitigation effectiveness vs. burden
3	Options for mitigating flexibility
4	Options for OD and GSC governance changes
5	Current and alternative data collection methods

Outcomes and Impacts	Develop data-driven recommendations to improve return-on-investment of current FOCI review and mitigation approaches, supporting efficient oversight of FOCI determinations

Figure 5. Proposed FOCI Study Objectives

Assess Effectiveness of Identifying and Prioritizing FOCI Risks. Evaluate the new SF-328’s effectiveness in identifying risk, as well as the usability of the new instructions. After about a year of implementing the new form, it is important to evaluate whether the new SF-328 effectively serves its purpose. Many companies have submitted the new SF-328 and DOW should not wait for Section 847 implementation to evaluate the form’s effectiveness. More specifically, the proposed study would identify error rates and specific areas where errors are most avoidable and frequent, and whether the new instructions improve the percentage of forms returned to industry in the initial triage phase. Study questions should include: Does the new form bring risks to light that would have been previously missed? Is the information requested effectively capturing the content DCSA requires for better risk reviews?

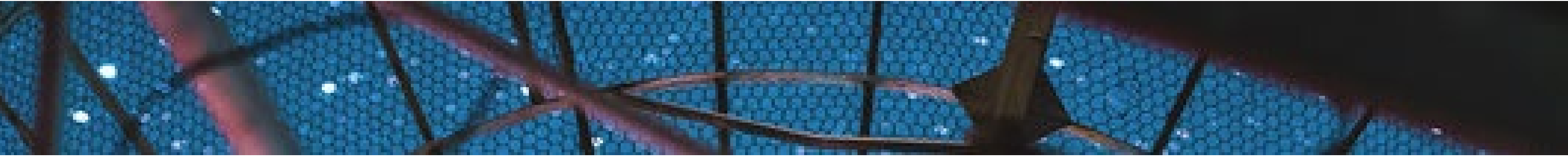
By using data to better understand the utility of this information to identify FOCI risks, DCSA can determine whether the new SF-328 captures the most important data while minimizing extraneous content to ultimately streamline industry information collection and DCSA review time. Further, the proposed study would provide initial insight that DCSA could leverage in establishing a data-driven oversight system to continuously evaluate the FOCI process, data gathered, and effectiveness in mitigation efforts. Lastly, the proposed study should identify and leverage existing methodologies from other USG initiatives for collecting beneficial ownership data, aiming to minimize the reporting burden on companies while maintaining efficiency and effectiveness.

Assess Mitigation Effectiveness vs. Burden. Assess relative effectiveness of mitigation options in reducing risk and whether they justify the implementation burden on industry. Given the cost and burden of FOCI mitigations, a study must evaluate whether DCSA is leveraging the lightest measures to effectively address FOCI risk. Interviewees describe the mitigation structure as content neutral on many company nuances, and funnels companies into well-defined categories based on clearance levels rather than implementing a flexible approach. Interviewees questioned why many long-held successful FOCI-mitigated companies are still required to overcome numerous obstacles even without incidents, and as one interviewee noted, "*FOCI policy treats allies as adversaries, reducing innovation and trust.*" The proposed study could assess an allied-owned mitigation path for trusted entities that emphasizes risk-based reviews over checklists. The proposed study would need to determine if objective, risk-based criteria (e.g., treaty allies with reciprocal security assurances, statutory frameworks) can manage risk and reduce duplication of effort.

Identify Options for Mitigation Option Flexibility. Enable transparent, risk-based mitigations. Several interviewees noted the FOCI process lacks transparency about the identified FOCI risks. For FOCI-mitigated companies, it is not always clear the risk that mitigations and implementation mechanisms are addressing and how they are meaningfully addressing that risk. In absence of understanding the purpose and intent, some companies considered DCSA to be using templated techniques to "check a box" without truly addressing FOCI risk and bolstering security. Interviewees described the DCSA culture as "wed to their playbook" without flexibility to deal with nuances of different company structures. The industry feedback conflicts with DCSA's FOCI Mitigation Agreement webpage,[97] which notes "mitigation customization may be required by DCSA based on the unique needs of each business." The proposed study must examine areas where flexibility can be increased in mitigation plans to better address the nuances of different companies leveraging a risk-based approach. In the short-term, industry would benefit from DCSA clearly articulating why mitigations and instruments are selected, and how templates will assist with addressing risk. By articulating intent, companies will be better able to justify investment in risk mitigation options, resulting in more effective corporate leadership implementation and motivation to support security.

Identify Options for OD and GSC Governance Changes. Enable DCSA to use data to evaluate and update ODs and GSC roles, responsibilities, and qualifications including options to empower the roles with more decision-making authority. The proposed study will allow the DIB to move at the speed of industry and mission, rather than relying on government for approvals of low-risk efforts. Interviewees noted previous DSS research to strengthen the framework and partnership of ODs, published in a 2018 White Paper, *Partnering with Outside Directors and Proxy Holders to Strengthen FOCI Boards*. However, the extent to which findings and recommendations were implemented remain unclear. The proposed study would benefit from a re-evaluation of this previous effort.

[97] DCSA (n.d.). *Mitigation Agreements.* Source: https://www.dcsa.mil/Industrial-Security/Entity-Vetting-Facility-Clearances-FOCI/Foreign-Ownership-Control-or-Influence/Mitigation-Agreements/



Compare Current and Alternative Data Collection Options. Examine past incidents to determine how they would have been prevented by the new SF-328 and mitigations, and whether the form has had any deterrent effect on DIB participation. Options should be examined for alternative data collection methods which do not require as much manual input from companies.

Assess FOCI Process Across non-DOW Cognizant Security Agencies (CSAs). Review how other CSAs follow FOCI procedures. All CSAs follow FOCI procedures as documented in the NISPOM; however, specific processes vary at the implementation level. Based on FAST Study questionnaire data, six respondents reported no reciprocity in FOCI determinations across CSAs, whereas only three respondents indicated successful reciprocity. Additionally, interviewees noted FOCI process timelines vary across CSAs. Given the implementation variance across CSAs, the proposed study should conduct an analysis of FOCI processes across other non-DOW CSAs to identify lessons learned, leading practices, and viable areas for transition to the DOW and DCSA process. Analysis should examine specific processes such as data collection, review, decision-making, mitigation design and approval, and oversight.

FOREIGN OWNERSHIP, CONTROL, OR INFLUENCE (FOCI) INDUSTRY CHALLENGES

FOCI Review Process

1. SF-328 Complexity and Inefficient Review Process
2. Understanding the New SF-328

FOCI-Mitigated Company Experience

3. Negative Perceptions of FOCI-Mitigated Companies
4. Delays in Finalized FOCI Mitigation Agreements
5. Ineffective Use of Outside Directors and Government Security Committees

Supplemental FOCI Documentation and Templates

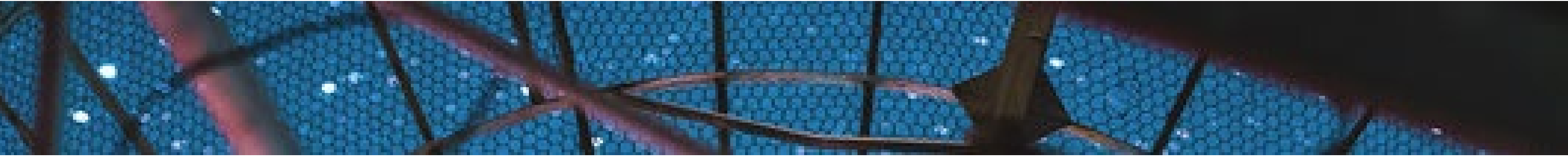
6. Need for Modernized Electronic Communications Plans
7. Burdensome Affiliated Operations Plan
8. Outdated Templates and Guides
9. Duplication Between ECP and CMMC

NDAA Section 847

10. NDAA Section 847 $5M Threshold Remains Undefined
11. NDAA Section 847 Implementation Guidance Woefully Needed

Modernizing FOCI Approach

12. Current FOCI Approach is Outdated



SAFEGUARDING OF CLASSIFIED AND SENSITIVE INFORMATION

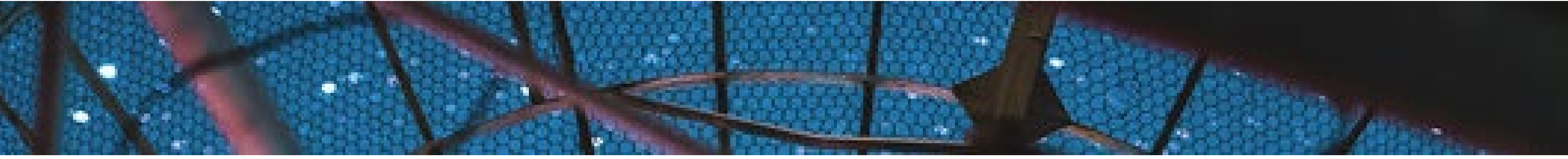
> *"We would bid more classified work if we had predictable access to space. Right now, we can't afford to wait a year."* – Small to Medium-sized Company Industry interviewee

The NISP was designed for an era in which classified information was physically bounded and human-mediated. Information resided in discrete locations; safes, vaults, secured rooms, and moved through deliberate, observable actions such as document transfer or face-to-face exchange. Industrial security controls were, therefore, built around fixed perimeters, static facilities, and assumptions of slow, intentional information flow under direct human custody. Those assumptions no longer hold. Today's classified information is created, processed, and transmitted within dynamic, distributed digital systems where custody is shared, movement is continuous, and control is exercised through architecture rather than walls.

Today, classified and sensitive information are the continuous substrate of operations, flowing through model-based engineering environments, cross-domain data fabrics, Operational Technology (OT) networks, cloud-native mission systems, and globally distributed supply chains. A single analytic product may be assembled from dozens of sources, fused across multiple domains, and then decomposed into smaller pieces to support targeting, logistics, training, and sustainment. The same core data informing warfighters at the tactical edge also lives in contractor development environments, test range enclaves, or multinational coalition networks.

The policy governing classified information, systems, networks, and facilities has historically prioritized securing physical documents over adapting to the realities of digital or non-paper formats. While the NISP, later codified in 32 CFR Part 117 (NISPOM), along with related issuances such as DODM 5200.01, DODI 5200.48, DAAPM, the DCSA Authorization and Assessment Guide (DAAG, recently released), the Joint Special Access Program Implementation Guide (JSIG), ICD 705, and others, provide a comprehensive framework for classifying information, accrediting systems and facilities, and safeguarding national security data throughout its lifecycle, the challenge lies not in the rules themselves but in their implementation. In practice, the processes designed to enforce these rules—classified systems and classified facilities—continue to operate as though information remains stationary, paper-based, and slow-moving, failing to fully account for the dynamic and fast-paced nature of modern information exchange. This outdated approach risks undermining the effectiveness of safeguarding national security data in an increasingly digital world.

In 2025, industry attempting to do routine classified work continues to encounter multi-year-long SIPRNet provisioning timelines, unpredictable SCIF accreditation outcomes, regionally divergent interpretations of the same standard, and cross-domain solutions (CDSs) that must be re-engineered afresh for each new program. The FAST Study questionnaire responses indicate the pain is trending worse: 47% of the DIB reported SCIF initial accreditation timelines are four months longer now than in FY21. The DIB spends months navigating access to networks and



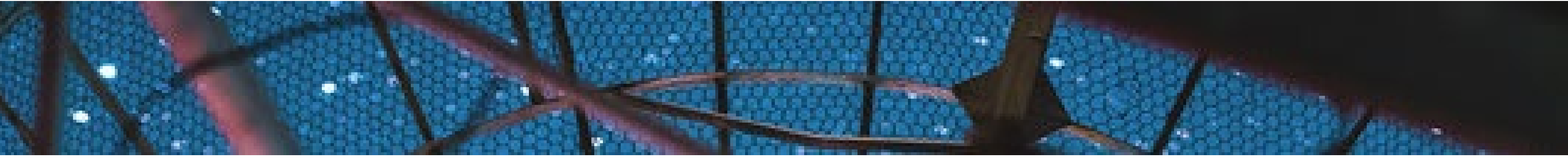
facilities before even beginning the work the government is paying them to do. As many interviewees framed it, "…(everything) is sequential, SCIF, then networks, then Authority to Operate (ATO). By the time you're ready, the schedule is blown." Questionnaire data also shows why the "ATO step" prevents the work from starting, 15 DIB companies reported that SCI system accreditations average 6.67 months with a long tail (up to 36 months), and "longest time-to-accredit" for SCI averaged 13.67 months with a longer tail (up to 60 months).

> *"You can't support the mission unless you have people, places, and things, all three in harmony."*— Large Prime interviewee

The FAST Study explicitly documented this tension of having people, places, and things ready. Across interviews, questionnaires, and document reviews, a consistent picture about classified and sensitive information risk, classified systems and networks, and classified facilities emerged:

- Programs routinely design systems, select architectures, and award contracts before they know what must be protected, at what level, and where that protection must live.
- Classification and CUI guidance arrives late (if at all), varies by MILDEP and region, and often contradicts itself when it crosses organizational seams.
- Classified systems and networks and SCIFs are treated as bespoke, one-off projects rather than reusable infrastructure, leading to repeated rework and uneven expectations.
- Policy is applied inconsistently by oversight bodies and is personality dependent. Industry has learned to navigate the lack of predictability. DCSA review and DIA accreditation bodies apply the same policies differently depending on zip code, creating a "geography of interpretation" that industry has learned to navigate but cannot predict. One interviewee summed up this experience with DCSA, *"We've had to redesign our security approach multiple times, not because policy changed, but because the reviewer changed."* The FAST Study questionnaire data reinforces this variability where only 43% of DIB said requirements were applied similarly across their last few DIA SCIF initial accreditations and 40% said DIA SCIF audits were applied similarly, meaning a large minority experienced reviewer-driven divergence even when "the standard" did not change.

The result is an **ecosystem in which the rules exist, but the consistent implementation of the rules does not exist.** Classified systems, networks, and facilities that should function as enablers instead become friction points. Programs lose months to provisioning and accreditation, instead of innovating for the warfighter. Workarounds, both technical and procedural, proliferate at the edges of the system, increasing handling and cyber risk in exactly the places the current framework was designed to control. Small and medium-sized companies are deterred from entering or staying in the classified market because they cannot absorb the overhead or uncertainty. Clearly understanding the full implications and solving this challenge matters operationally, not just administratively. When a SCIF sits idle waiting on an unpredictable accreditation, development and analysis stall. When metadata and markings break at each boundary crossing, automation, AI triage, and cross-domain fusion cannot be trusted and must be replaced with manual intervention.



When SIPRNet access for a company takes over a year, a capability that could have been fielded in months, arrives after the threat picture has shifted. For the warfighter, these delays are not abstract, they show up as missing data, deferred upgrades, and slower decision cycles in contested environments.

The FAST Study, therefore, treats **Classified Systems and Networks** and **Classified Facilities** not as legacy compliance topics, but as two of the most consequential bottlenecks in the modern protection of classified and sensitive information. The policies that govern them are mature; the missions that depend on them are urgent; yet the way they are implemented remains uneven, slow, and misaligned with how information actually moves in 2025.

The challenges in this section do not require a full policy rewrite or breaking down the existing frameworks. Instead, they expose where implementation is structurally failing, where guidance arrives too late, where markings and metadata cannot be trusted across systems, where cross-domain patterns are reinvented for each program, where SCIF and SIPRNet access depend more on region than on requirement; and the FAST Study identifies concrete actions the Department can take to turn classified information, systems, networks, and facilities from constraints into genuine enablers of successful mission execution. While the FAST Study underscores that many implementation rules still treat information, networks, and facilities as if they were stationary (i.e., on paper), it also recognizes that this is only one part of the challenge. Persistent shortfalls in prioritization, staffing, funding, and integration of security into the acquisition process have compounded these structural flaws and must be addressed in parallel for modernization to succeed.

Classified and Sensitive Information Risks

31) Programs Begin Without CPI, CTI, CUI and Fail to Establish Early, Authoritative Protection Plans

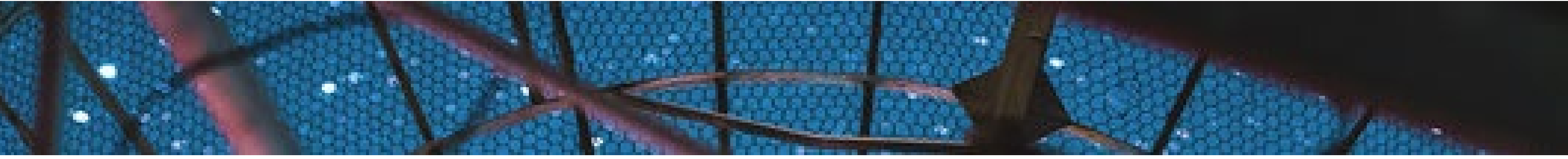
> *"We don't know what's CPI until we're halfway through design. That's too late to protect anything."* — Industry interviewee

Challenge

Warfighter programs routinely move through key acquisition milestones, release solicitations, make subcontracting decisions, and lock in early system architectures before establishing authoritative Controlled Program Information (CPI), Controlled Technical Information (CTI), Controlled Unclassified Information (CUI), and classification boundaries. In the absence of early, explicit protection direction required by DOW policy[98] and advised by DOW implementation guidance,[99] protection architectures become reactive, inconsistent, and costly to correct. DOW policy envisions a disciplined, front-loaded sequence in which CPI is identified early, CTI is

[98] DOD (2021). *DOD Instruction 5000.83: Technology and Program Protection to Maintain Technological Advantage*. Source: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500083p.pdf

[99] OUSD(R&E) (2022). *Technology and Program Protection (T&PP) Guidebook.* Source: https://rt.cto.mil/wp-content/uploads/2025/05/TPP-Guidebook_Jul2022_DOPSR-approved_Released.docx-1.pdf



derived from CPI, classification decisions follow technical risk, and these determinations shape acquisition planning and system design. In practice, FAST Study interviewees consistently stated that programs almost never follow this sequence.

CPI analyses, Security Classification Guides (SCGs), Program Protection Plans (PPPs), and CUI annexes frequently arrive after key decisions have already been made during pre-Milestone A and B planning, early RFP drafting, digital engineering environment setup, and teaming arrangements. Without early CPI and CUI direction, DOW DIB engineering teams make foundational design decisions without knowing what information actually matters. As one interviewee summarized, *"We make design decisions blind because the program has not told us what actually matters yet."* In addition, subcontractors often begin preliminary work without clarity on whether artifacts they generate will ultimately be treated as CUI, CTI, or classified.

The late arrival of PPPs, SCGs, and CUI annexes forces DIB contracting staff, engineers, and partners into guesswork. Interviewees consistently reported that early RFP sections rely on generic or placeholder security language that does not clearly identify applicable information categories, required markings, or expected system accreditation levels. Oversight organizations interpret these gaps differently, producing inconsistent regional and MILDEP-level expectations.

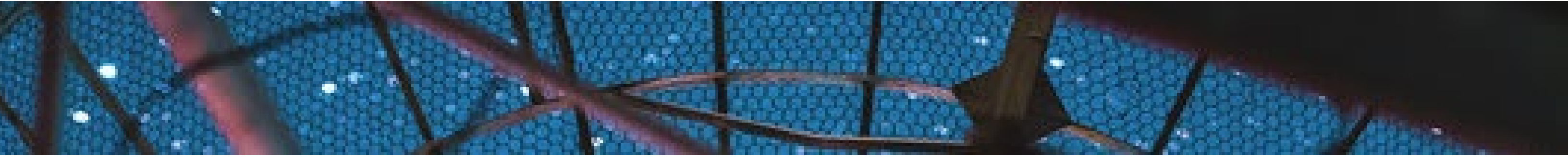
> *"The SCG showed up six months after award. Everything we designed had to be rebuilt to match requirements we did not know existed."* – Industry interviewee

FAST Study interviews consistently described that this cycle of rework is structural rather than episodic. Interviewees described that program offices often lack the mandate or operational discipline to generate early protection artifacts that meaningfully guide acquisition strategy and technical baseline formation. When program offices fail to generate those early protection artifacts, the result is an enterprise that builds systems and networks before defining what must be protected, why it must be protected, and to what standard. This outcome directly contradicts DOW policy intent. CPI and CTI identification are not compliance tasks; they are foundational design drivers.

These late and incomplete protection decisions also degrade execution. Acquisition personnel and program staff frequently issue contradictory or technically infeasible handling instructions, not due to policy disagreement, but because of limited applied understanding of how CUI and classified information are handled in modern toolchains and environments. One industry interviewee observed that acquisition personnel *"do not understand the tools we are asking industry to use,"* resulting in mismatched expectations for enclaves, transmission channels, and subcontractor environments.

> *"We would gladly follow strict rules. Just make them consistent, visible, and tied to real risk. Right now, CUI feels like classified without the map."* – Industry interviewee

Government-provided guidance often conflicts with observed government practice, leaving industry to create its own internal training and interpretation to keep programs moving. This



shadow guidance varies widely in accuracy and quality, particularly among small businesses and subcontractors. In some cases, MILDEPs effectively treat CUI as classified by default. As one interviewee described, "*Some DOW elements treat CUI as SECRET by default and then demand SF-86-level checks for CUI access.*"

Throughout interviews and questionnaires, DIB prime contractors outlined how delays in receiving PPPs, SCGs, and authoritative CUI guidance directly impacted their ability to flow requirements to subcontractors. In the absence of timely guidance, subcontractors lack clear CPI, CUI, and classification boundaries, marking rules, and need-to-know determinations. This drives either over-protection that increases cost and schedule risk or under-protection that increases mishandling and disclosure risk. The cumulative effect is systemic risk across the DIB supply chain, reduced competition, delayed delivery, and uneven security outcomes.

Recommended Government Action

Program Protection Baseline (PPB). OUSW(A&S) should establish a mandatory PPB as an acquisition gating artifact. The PPB must be completed and approved prior to acquisition strategy approval and prior to any public release of solicitation materials. The PPB is not advisory and may not be deferred or "refined later." Programs may not finalize or release RFPs, engage industry, or authorize early technical work until the PPB is documented, adjudicated, and approved.

OUSW(I&S) should define the authoritative protection content of the PPB, and the DOW CIO should ensure traceability into system security and RMF execution. At a minimum, the PPB must include: an initial CPI analysis; a preliminary CTI determination; a draft SCG; a CUI annex aligned to DODI 5200.48; and an early-stage PPP framework. These artifacts must function as binding, government-furnished design inputs that inform system architecture, contracting strategy, teaming decisions, and subcontractor flowdowns.

The PPB must serve as the authoritative upstream source for downstream security artifacts and decisions, including final PPP development, RMF control selection and inheritance determinations, System Security Engineering (SSE) requirements, and subcontractor security flowdowns. Programs may not reinterpret, substitute, or delay these determinations downstream without formal adjudication and approval through the same authority that approved the PPB. Government delivery of PPB artifacts should be treated as a prerequisite for security-dependent design reviews, architecture approvals, and major technical milestones, ensuring protection decisions are validated before irreversible design commitments are made.

PPB Acquisition and Contract Mechanism. OUSW(A&S), in coordination with OUSW(I&S), should require acquisition and contract mechanisms that formally recognize the PPB, PPP, SCG, and authorized CUI guidance as Government-furnished prerequisites upon which contractor performance, compliance, and delivery timelines depend. Solicitations and contracts should explicitly designate these protection artifacts as government-controlled dependencies, and must include provisions stating that delays, incompleteness, or contradictions in government-provided security guidance constitute excusable, non-attributable impacts on contractor performance. This will codify government accountability without transferring risk to the DIB.

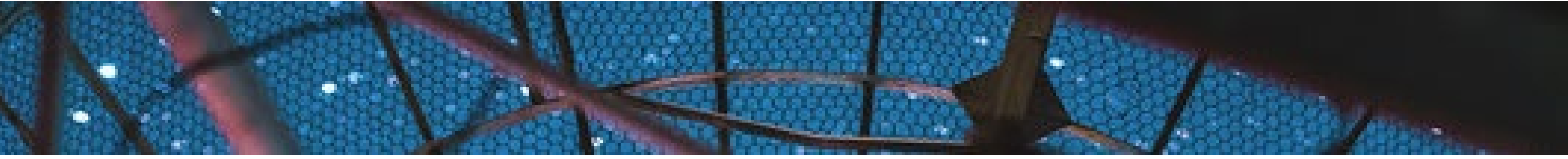
Where required protection artifacts are late, incomplete, or internally inconsistent, contractors must be explicitly permitted to defer dependent technical, security, or programmatic deliverables without penalty, including without adverse impact to CPARS evaluations, award fee determinations, incentive structures, or compliance ratings. Contractors may not be held responsible for non-performance or schedule impact that is causally attributable to the government's failure to provide authoritative protection guidance. Programs should be required to document the timeliness and completeness of government-furnished protection artifacts and treat delays as government-caused execution risk, rather than contractor deficiency. Oversight organizations must be prohibited from assigning negative contractor performance ratings or fee impacts for deliverables that depend on undelivered or delayed government security artifacts.

This construct establishes reciprocal accountability while preventing the transfer of government non-performance risk onto industry, reducing disputes, improving trust, and ensuring that early protection guidance functions as a prerequisite to execution rather than a post-award correction. By formalizing protection artifacts as government-furnished prerequisites and providing explicit safe-harbor provisions, this approach reduces disputes by eliminating ambiguity about responsibility for delays and preventing after-the-fact attribution of government non-performance to contractors.

Timeliness of PPPs, SCGs, DD-254s, and CUI Guidance. DOW should ensure timely execution-phase delivery and flowdown of approved protection artifacts. Consistent with the PPB, DOW should provide approved PPPs, SCGs, DD-254s, and authorized CUI guidance to prime contractors no later than contract award, and update them within defined, enforceable timelines as program conditions evolve. DOW should also provide prime contractors with approved need-to-know extracts authorized for immediate release to subcontractors, enabling protections to be flowed down and implemented correctly from the start of performance. Contracts should explicitly recognize subcontractor protection implementation timelines as dependent on government delivery of these artifacts, and primes may not be penalized for downstream delays caused by late or incomplete government guidance, leading to execution-focused protection flowdown to subcontractors.

Acquisition security professionals should track the timeliness of PPP, SCG, DD-254, and need-to-know delivery to subcontractors as an execution risk metric and require corrective action when government-provided guidance is late or incomplete. This execution discipline ensures that early protection decisions established through the PPB are implemented consistently across all tiers of the supply chain, rather than degrading through delay, reinterpretation, or informal workarounds during contract performance.

Government CUI Training. DOW should require applied, role-specific CUI training that enables consistent execution of authoritative CUI policy across acquisition, security, engineering, and program management environments. Training should focus on real-world failure modes identified in the FAST Study, including mismarking, improper elevation of CUI to classified handling, infeasible dissemination instructions, and misunderstanding of approved transmission and enclave models. Training must be tailored by role and aligned to the authoritative CUI Marking and Dissemination Profile. Modules should explicitly address how CUI is handled in modern



toolchains, subcontractor environments, and cross-MILDEP workflows, and should be updated when systemic misapplication is identified through government accountability mechanisms. This will raise the overall workforce competency to apply CUI.

Impact for Warfighter

When CPI, CTI, CUI, and classification decisions are made early, systems and platforms will be built on stable foundations. Engineering teams will not have to redesign architectures, subcontractors will not have to pause work waiting on access to needed data or environments, and capability delivery to operational forces schedules will not slip. At a strategic level, early protection will guard sensitive technologies from adversary exploitation, develop security trust in acquisition processes, and increase competition by enabling entry by new companies with less funding to absorb government redesign cycles. The cumulative effect is lower cost, faster fielding, better end-to-end security, and increased long-term military advantage. Consistent early delivery of PPPs, SCGs, and authorized need-to-know extracts will enable prime contractors and subcontractors to implement protections from program start. Correct protections will reduce rework, cost, and schedule delay due to unintentional security misconfiguration while lowering the risk of mishandling and unauthorized disclosure. The result will be faster, more predictable delivery of capabilities, strengthened supply chain assurance, and higher mission readiness, so warfighters receive needed technologies and data on time and with greater confidence in their integrity.

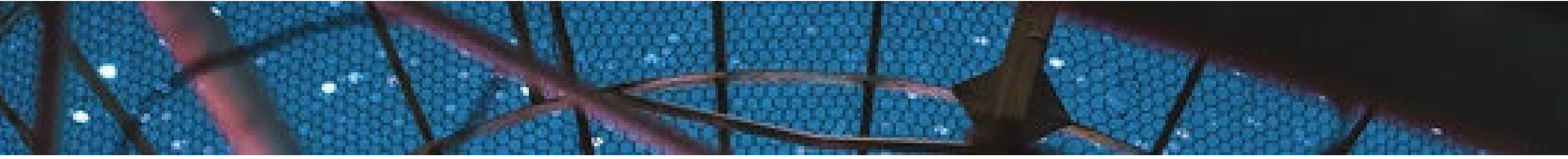
32) CUI Policy Implemented Inconsistently Across DOW

> *"The government sends us unmarked CUI, unencrypted, and then holds us to the standard they don't follow."* – Industry interviewee

Challenge

Fifteen years after the creation of the CUI program, USG-wide implementation is nonexistent and DOW's implementation remains fragmented. MILDEPs interpret CUI categories differently, apply markings inconsistently, and often impose requirements with no policy basis. Interviewees described instances where their company was explicitly directed by DOW to treat CUI as Secret or Top Secret, or required CUI-only work to occur inside SCIFs. The transition from FOUO to CUI remains uneven across government and DOW, producing what one industry interviewee called "*31 flavors of implementation*."

> *"If we handled CUI the way the government sends it to us, we'd have an incident."*
> – Industry interviewee
>
> *"One section said CUI, another said FOUO, and the attachments had neither marked. We had to assume the strictest case to be safe."* – Industry interviewee



> *"They told us it was CUI, but then required it to be produced in a SCIF. There was no SCG, just 'that's how we do it here."* – Industry interviewee

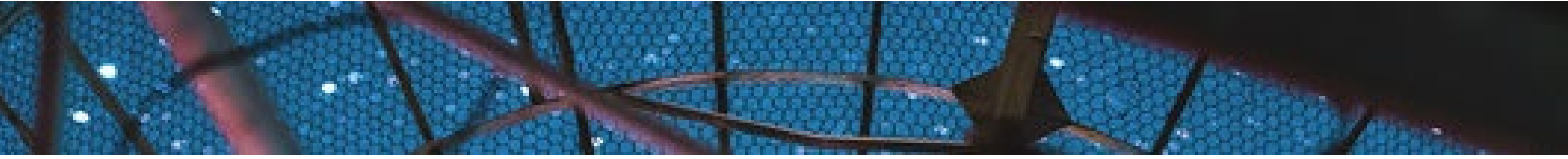
Based on interviews, DOW government employees frequently mishandle CUI when sending it to DIB companies. Examples from FAST Study data include sending CUI to DIB companies through noncompliant channels (e.g., unencrypted), or through appropriate channels (e.g., DOW SAFE) but unmarked or improperly marked. Government mishandling of CUI when engaging with DIB companies has led to situations where government actions would have resulted in cyber incidents and security violations if performed by a DIB employee. In some cases, interviewees noted their companies had technically experienced cyber incidents due to DOW sending CUI to systems not accredited for handling such information, or because the CUI was incorrectly marked leading to improper handling. There is a concerning disparity in standards, where the DIB is held to higher expectations for safeguarding CUI, while government practices fail to meet those same standards, creating vulnerabilities and risks in the process. One large DIB interviewee described this well *"CUI training exists and the definition is clear; issues are mostly inconsistent government behavior."*

In addition, interviewees described multiple instances in which government acquisition personnel inserted contradictory or technically infeasible CUI handling instructions into RFPs, such as requiring CUI to be handled as classified or mixing CUI and FOUO requirements, reflecting inconsistent MILDEP-level interpretations rather than policy deficiencies. The result of the CUI inconsistencies and unequal expectations is a structurally inconsistent environment creating confusion, rework, unnecessary cost, and avoidable risk for the DIB. Inconsistent CUI implementation delays acquisition timelines, limits effective information sharing, and forces companies to rebuild environments or re-mark data mid-performance. These disruptions reduce industry participation, particularly among small businesses, and weaken the resilience and speed of DIB. Ultimately, the warfighter receives capability later and at higher cost due to avoidable administrative and technical rework.

Recommended Government Action

OUSW(I&S) should issue a binding Department-level policy instrument that mandates a single, authoritative CUI Marking and Dissemination Profile applicable across MILDEPs. The policy instrument should require uniform use of defined CUI categories, marking formats, dissemination controls, and approved transmission mechanisms, and should explicitly prohibit MILDEP-specific reinterpretations or continued reliance on legacy FOUO constructs. The profile should align with DODI 5200.48 and be updated to reflect the final FAR Rule 2017-016.

OUSW(A&S) should enforce use of the authoritative CUI profile through acquisition entry points**.** Programs should be required to include explicit CUI determinations and marking guidance derived from the authoritative profile in all relevant solicitation packages. Solicitation materials that rely on generic, placeholder, or contradictory CUI language should not proceed to release until corrected.



OUSW(I&S), with support from the DOW CIO, should operate a Department-wide mechanism to identify, adjudicate, and correct government-side CUI mislabeling and mishandling. This mechanism should allow DIB companies to report persistent government errors anonymously, require MILDEP-level response and correction within defined timeframes, and track recurrence to identify systemic divergence rather than isolated mistakes.

Industry interviewees noted that the CUI program is not consistently applied across the USG. A USG-wide directive is necessary to establish uniform CUI handling obligations and enforcement mechanisms for government personnel (e.g., NARA/ISOO), ensuring a consistent government-wide CUI program. Currently, a DODIG Report[100] identified that ISOO's role was complicated by the policy reform process, contributing to delays. A 2022 National Security Council Memorandum[101] initiated a review of Executive Order 13556,[102] effectively placing many agencies' CUI efforts on hold. As of 9 April 2024, for example, only 40 agencies had CUI policies and only 38 agencies adopted safeguarding practices.[103] The Department in collaboration with NARA/ISOO should advocate for a government-wide directive via an OMB directive or Executive Office of the President (EOP) or Presidential Memorandum that establishes parallel obligations, reporting, and consequences for government personnel handling of CUI. Government service members and civilian employees should be held to the same marking, dissemination, and handling standards imposed on the DIB, with recurring government-side violations addressed through existing accountability and oversight mechanisms rather than treated solely as training issues.

Impact for Warfighter

These actions enable the warfighter by streamlining and standardizing government's operational expectations of the DIB and reducing the likelihood of CUI being mishandled in transmission from government to industry. By minimizing administrative and technical disruptions from CUI mishandling, the DIB can more consistently focus on delivery to ensure the warfighter receives more timely, cost-effective capabilities to support mission success. The warfighter can also have greater assurance that capabilities delivered to them are less likely to have been compromised through CUI mishandling during the acquisition lifecycle.

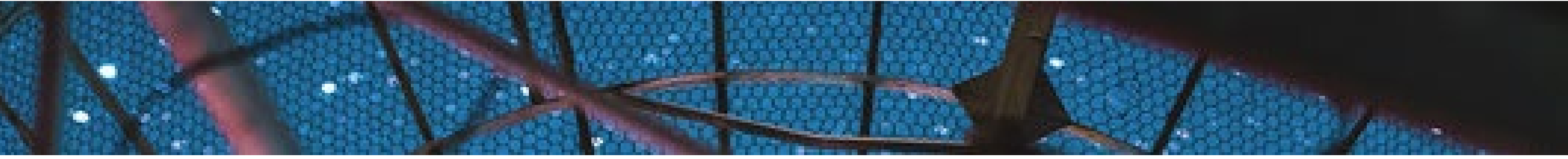
Company Experience: A company reported that a DOW government contracting office directed its personnel to mark nearly all outbound email as CUI, regardless of content. The interviewee emphasized that most of the information clearly did not meet the CUI definition, but the directive forced routine correspondence to be handled as controlled information. This practice increased administrative burden, slowed communication, and undermined confidence that CUI markings conveyed meaningful distinctions about sensitivity, increasing the likelihood that truly sensitive information would be overlooked amid over-marking.

[100] DODIG (2023). *Audit of the DOD's Implementation and Oversight of the Controlled Unclassified Information Program (DODIG-2023-078).* Source: https://media.defense.gov/2023/Jun/01/2003234002/-1/-1/1/DODIG-2023-078.PDF

[101] Cited in: ISOO (2022). *CUI Notice 2022-01: Executive Agent Guidance Regarding White House National Security Council (NSC) Memorandum, "Initiating a Process to Review Information Management and Classification Policies," June 2, 2022.* Source: https://www.archives.gov/files/cui/documents/cui-notice-2022-01-09.06.2022.pdf

[102] The White House (2010). *Executive Order 13556—Controlled Unclassified Information.* Source: https://www.govinfo.gov/content/pkg/DCPD-201000942/pdf/DCPD-201000942.pdf

[103] ISOO (2023). *Annual Report to the President*. Source: https://www.archives.gov/files/isoo/reports/isoo-fy-2023-annual-report.pdf



33) Lack of Standardized and Practical CUI Training Risks Mishandling

Challenge

CUI training across DOW and industry remains inconsistent, outdated, and disconnected from day-to-day implementation challenges. Consequently, personnel at all levels, including PMs, KOs, DIB employees, and DIB subcontractors, frequently misunderstand or misapply CUI requirements. While DODI 5200.48 establishes rules governing CUI, training on those rules is fragmented and often inadequate. DOW training modules differ by MILDEP, are infrequently updated, and rarely address the mismarking, over-restriction, and dissemination failures encountered daily by the DIB.

Interviewees reported repeated cases in which government staff issued contradictory or technically infeasible CUI instructions, not out of policy disagreement but from a lack of comprehension. One interviewee noted that acquisition personnel *"don't understand the tools we are asking industry to use,"* resulting in mismatched expectations for enclaves, transmission channels, and subcontractor environments. At the same time, industry cannot rely on government-provided training because it often conflicts with observed government practice. Consequently, industry has produced its own training material, leading to variation in accuracy and quality, especially among small businesses and subcontractors.

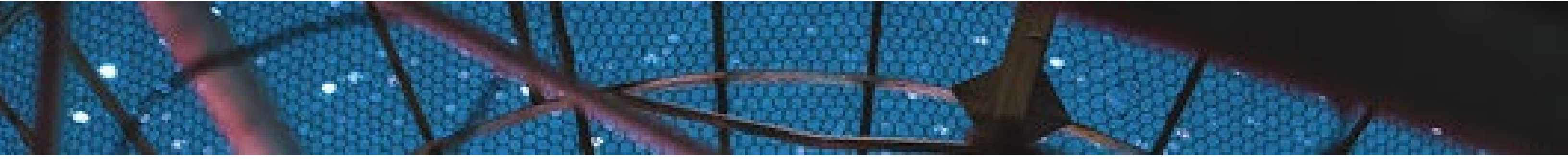
Operationally, unclear or contradictory dissemination expectations hinder joint collaboration and data exchange. Strategically, inconsistent training undermines trust in the CUI framework and increases the long-term risk of mishandling sensitive defense information. These gaps reflect a workforce competency issue rather than a policy inconsistency. Personnel lack the practical, applied understanding necessary to implement CUI correctly.

Recommended Government Action

OUSW(I&S) should establish standardized, mandatory CUI training baseline applicable for industry. This training must incorporate real-world mismarking examples, address common misconceptions (including the improper elevation of CUI to classified handling), and provide tailored modules for acquisition personnel, technical performers, and project management. Training should explicitly cover dissemination channels, marking rules, subcontractor flowdown expectations, and MILDEP-to-MILDEP interoperability issues. DOW already requires government personnel to complete mandatory annual CUI training. The current training should be reviewed and updated to include the recurring issues described above. In addition, DOW should assess whether CUI training should be as detailed and require practice like current classified handling and marking training due to its increased importance and high level of confusion.

Impact for Warfighter

Standardized and mandatory CUI training across government and industry will improve the consistency of requirements application, reducing delays and miscommunication that affect the delivery of critical capabilities to warfighters. Enhanced dissemination practices and interoperability could strengthen joint collaboration and data exchange, improving operational effectiveness. Overall, these actions aim to better protect sensitive defense information, fostering trust and supporting warfighters in executing missions more effectively.



Classified Facilities

34) New Entrants and Subcontractors Face Reduced and Unpredictable Access to Classified Space

Challenge

The USG and DOW understand the importance of physical requirements to handle and process classified information. Yet, DIB subcontractors, particularly small and medium-sized businesses, face inconsistent and often restrictive access to classified facilities controlled by prime contractors or government organizations. These barriers limit competition, delay performance, and create structural disadvantages within the DIB. The goal is to maintain the minimum requirements to protect classified information and execute those requirements more efficiently and effectively.

The FAST Study found a consistent pain-point for subcontractor's is access to SCIF spaces. Interviewee experiences varied widely based on prime contractor policies, government facility availability, and regional DCSA practices. Many DIB subcontractors reported waiting months for facility access even when their personnel or entity held the appropriate clearances. Some prime contractors restrict access based on internal space constraints, security interpretations, or business considerations, leaving subcontractors unable to perform required classified work and delaying contract start and thus delivery.

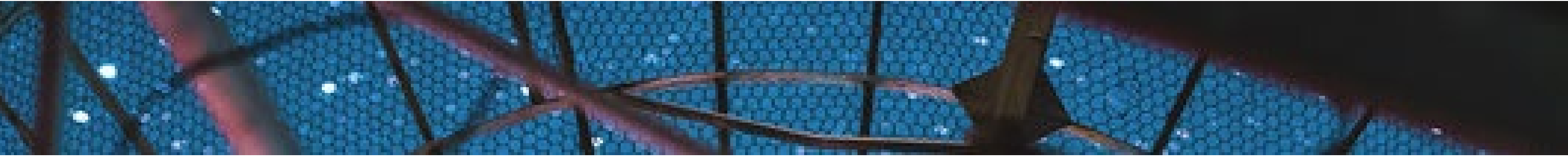
Small businesses are disproportionately affected. When SCIF facility access is denied or delayed, they cannot begin or complete contract performance, and their contribution to the warfighter's advantage is delayed. This challenge heavily discourages them from pursuing classified work and reinforces market concentration.

> *"If the prime won't let us into their SCIF, we have no way to do the work, even though the government awarded us the contract."* – Industry interviewee

Government program leaders or KOs typically do not require prime contractors to provide access-sharing plans, nor do they establish performance metrics governing classified facility availability. As a result, subcontractors have no recourse when access is limited, and the government has limited visibility into how access constraints affect performance or competition.

Recommended Government Action

OUSW(A&S) should require programs and prime contractors to develop and maintain classified facility access plans for subcontractors. These plans should identify available space, expected access levels, and procedures for scheduling or requesting access. The Department should use solicitation and contract requirements to incentivize and (where mission-appropriate) require prime contractors to share classified facilities with subcontractors. Solicitations and contracts should include evaluation factors and clauses that require prime contractors to develop classified facility-sharing plans for their subcontractors. The Department could also offer positive incentives to prime contractors who consistently share their space with subcontractors. These incentives could



be reflected in award fee measures and high CPARS ratings for meeting classified facility-sharing metrics, and allowing cost recovery for security staffing and access control that supports subcontractor use. OUSW(I&S) in its oversight capability should work with the DOW Office of Small Business Programs (OSBP) to collect data on subcontractor access delays, evaluate their impact on program performance, and require transparency when access constraints impede execution.

Impact for Warfighter

Reliable and predictable subcontractor access to classified facilities accelerates program execution and enables faster integration of innovative capabilities into operational systems. When qualified subcontractors can access required classified spaces in a timely manner, they can begin work as planned, contribute fully to mission delivery, and reduce delays in contract performance.

Strategically, consistent access-sharing practices expand participation across the DIB, strengthen supply chain resilience, and enable small and medium businesses to compete on performance rather than facility ownership. By reducing structural barriers to classified work, the Department can increase DIB competition, accelerate capability delivery, and ensure the warfighter benefits sooner from a broader range of technical solutions and expertise.

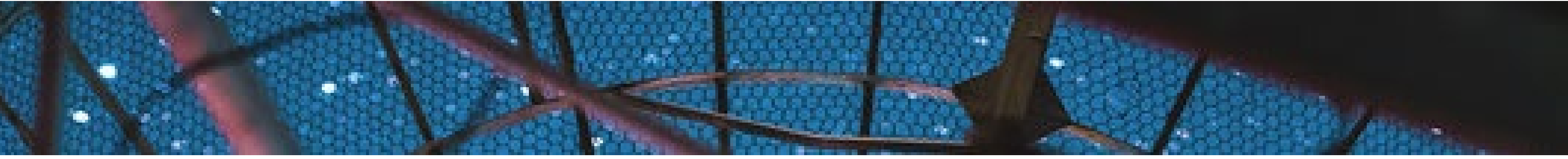
35) SCIF Accreditation Timelines Are Unreasonable

> "*DIA takes forever to get DIA accredited facilities*" – Industry interviewee

Challenge

FAST Study interviews with both prime contractors and subcontractors consistently identified SCIF accreditation as one of the most persistent facility-related bottlenecks affecting classified work under the NISP. Industry interviewees reported that DOW SCIF accreditation, managed by the DIA through its Facilities Enterprise Services (FES) function, frequently takes significantly longer than program schedules anticipate, even for facilities with relatively standard configurations. Interviewees reported accreditation timelines ranging from several months to over a year. Importantly, these timelines were not explained solely by differences in facility design or security posture. Instead, FAST Study interviews indicated that accreditation outcomes and timelines varied depending on the reviewing DIA FES region, workload distribution, sequencing of inspections, and interpretation of evidentiary requirements. Facilities built to similar designs and supported by comparable documentation were reported to experience materially different review durations based on the regional offices and inspectors involved.

As one industry interviewee stated, "*We submitted the same documentation that another site used, but our review took three times longer because the region asked for different evidence.*" Another interviewee described an accreditation that *"stalled for months with no explanation,"* leaving cleared engineers unable to begin classified work despite the facility being ready to operate.



Because accreditation timelines were difficult to predict, contractors reported challenges planning proposal schedules, staffing, and execution sequencing. In multiple interviews, companies described relocating personnel, shifting classified work to alternate sites, postponing sensitive discussions, or relying on temporary arrangements such as leasing short-term space or transporting cleared staff to distant accredited facilities. These workarounds introduced additional cost, increased schedule risk, and created operational inefficiencies, even in cases where facilities were ultimately approved without substantive changes.

Interviewees emphasized that the core issue was not unclear policy or insufficient standards. Rather, they attributed delays to inconsistent application, uneven throughput, and the absence of transparent timelines or predictable review expectations across DIA FES regions. As a result, DOW SCIF accreditation functioned less as a repeatable enterprise process and more as a variable, region-dependent gate, complicating execution planning and slowing the delivery of classified capabilities.

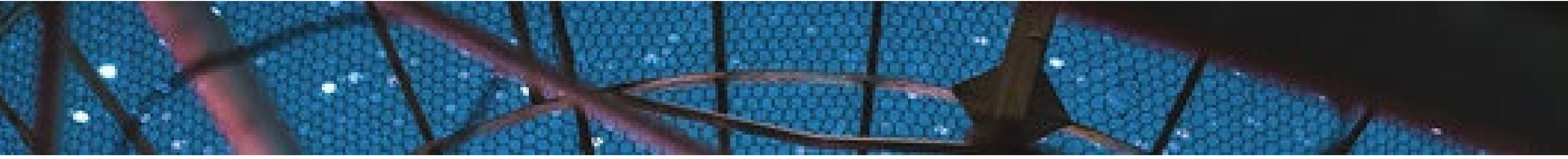
Recommended Government Action

Interviewees suggested that DOW SCIF accreditation authorities could be given back to the MILDEPs, who handled them until early 2021. However, SCIF accreditation was in part removed from the MILDEP-level due to DIB complaints about severely inconsistent accreditation requirements, processes, and timelines. Those MILDEP-level challenges would not be any different today. Instead, the OUSW(I&S) should double down on making DIA a fully staffed accreditation office with improved throughput by temporarily having MILDEP staff skilled at accreditation temporarily assigned to DIA until the backlog is remedied. At that point, DIA should be held accountable for having sufficient accreditors on staff and regionally based to handle all SCIF accreditations. OUSW(I&S) should implement time-bound accreditation milestones and require DIA to publish regional performance metrics to improve predictability. In addition, government programs should be required to incorporate SCIF planning earlier in the acquisition process and coordinate with DIA before contract award to validate feasibility. The Department should also create structured escalation pathways for contractors experiencing protracted delays without clear rationale, ensuring that accreditation bottlenecks do not stall critical mission work.

Impact for Warfighter

Predictable and timely SCIF accreditation enables faster initiation of classified development, testing, analysis, and sustainment activities that are essential to mission readiness. When accreditation timelines are transparent and consistently applied, programs can plan staffing, facilities, and execution sequencing with confidence, reducing delays in delivering classified capabilities to operational forces.

Strategically, reliable accreditation processes support modernization efforts, strengthen industry confidence in classified work, and lower the cost and friction of maintaining a capable and responsive industrial base. By ensuring SCIFs are accredited in alignment with program timelines, the Department improves execution discipline, accelerates capability delivery, and ensures the warfighter gains timely access to secure environments needed to support mission success.



36) DOW SCIF Reciprocity Exists in Policy but Fails in Practice

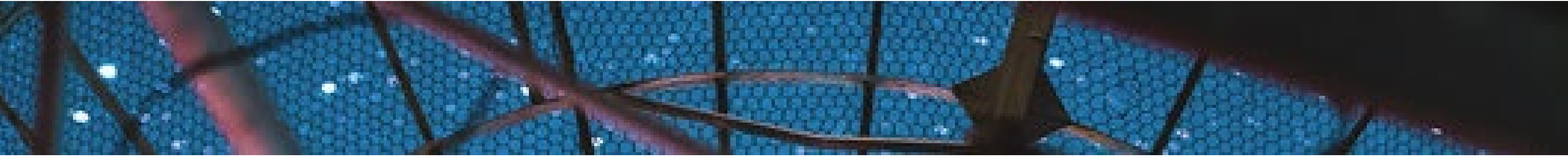
Challenge

The DOW has stated that there is sufficient SCIF capacity to meet current mission needs. The FAST Study team has not independently verified the statement. However, if this is accurate, the core challenge shifts from a question of aggregate SCIF capacity to one of distribution and access. In particular, the issue becomes whether SCIFs are geographically located where the work must be performed and whether appropriate, timely access to those facilities is made available to the organizations and personnel who need them. Although SCIF reciprocity is explicitly required under ICD 705 and DOW policy, DOW SCIF accreditations are frequently re-evaluated or challenged when DIB personnel move between MILDEPs or regions, causing unnecessary delays, re-inspections, and duplicative work.

The principle of reciprocity is clear: a SCIF accredited by one authorized body should be accepted as compliant by others, and a DOW SCIF accredited by DIA for one MILDEP should always be accepted as compliant by another MILDEP. In practice, however, reciprocity breaks down due to differences in interpretation, risk tolerance, documentation standards, and regional expectations. While policy recognizes reciprocity and co-use of accredited SCIF facilities, the same principle does not consistently extend to classified information systems and networks. In practice, contractors often face barriers to reciprocal access to networks such as JWICS, even when personnel are co-located within accredited SCIFs and meet identical clearance and need-to-know requirements. Differences in network configurations, access approval processes, and MILDEP-specific administrative controls introduce additional technical and procedural friction beyond that associated with facilities alone. As a result, cleared personnel may have physical access to a shared classified workspace but remain unable to access required systems or data, forcing redundant infrastructure, travel to alternate locations, or delays while network access is established. These challenges mirror those observed with SCIF reciprocity, and co-use are amplified by the technical and governance complexity of classified networks.

Industry interviewees described scenarios where a DOW SCIF that had been operating successfully for years under one MILDEP suddenly required revalidation when personnel from another MILDEP became involved. In other cases, facilities accredited in one region were questioned by officials in another, despite no change in configuration or usage. One FAST Study interviewee summarized the problem by stating, *“Reciprocity is something everyone agrees with on paper, but no one seems obligated to honor when the mission changes.”*

This dynamic introduces uncertainty into DIB facility planning. When DIB companies cannot rely on reciprocity, they must prepare for potential rework, gather redundant evidence, and accommodate unplanned inspections. For subcontractors, the problem is amplified because they may rely on multiple prime contractors or government sponsors, each with different expectations. The breakdown of reciprocity also discourages co-use, complicates multi-program integration, and contributes to stagnation in facility modernization efforts, as contractors prioritize avoiding reinspection risk over upgrading infrastructure.



Recommended Government Action

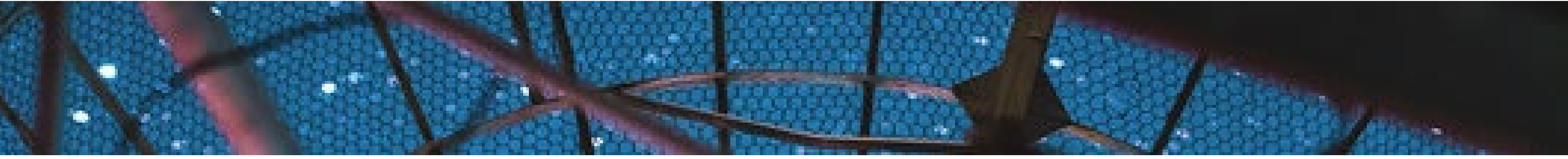
DOW SCIF Reciprocity Memorandum. The Department should request and advocate for the SecWar to issue a Department-level memorandum reaffirming and enforcing DOW SCIF reciprocity as the default expectation across all MILDEPs and regions. The memorandum should require standardized acceptance criteria, promote shared accreditation records, and reinforce inspector training that emphasizes honoring existing accreditations absent a documented, mission-specific risk justification. The view by all in DOW should start with "a SCIF is a SCIF."

The memorandum should be codified by OUSW(I&S) through updates to appropriate DOW Directives and Instructions. MILDEPs and regional offices should be required to document explicit justification whenever an existing DOW SCIF accreditation is not honored. A cross-regional escalation and adjudication mechanism should be established to resolve disputes rapidly and prevent unnecessary re-inspection and rework. The operating presumption across the Department should be that a SCIF accredited to ICD 705 standards or still accredited by DIA is accepted unless clearly justified otherwise.

OUSW(I&S) should issue guidance explicitly stating that effective SCIF reciprocity is a prerequisite for the success of Classified Infrastructure-as-a-Service (CIaaS) models. For CIaaS to operate competitively and at scale, SCIF accreditations granted to CIaaS facilities and systems must be honored across MILDEPs and regions without persistent re-adjudication. To reinforce this expectation, the Department should incorporate reciprocity-focused performance metrics into DOW-funded CIaaS pilots and broader SCIF governance. Metrics should include timelines for honoring existing accreditations and rates of challenged or re-opened accreditations. Without reliable reciprocity, CIaaS models will remain cost-ineffective and unable to support multiple programs, sponsors, and companies.

Accredited Classified Space Registry (ACSR). The Department, in coordination with DIA, DCSA, and GSA, should establish a secure, Department-wide catalog of accredited SCIFs and other classified facilities. The ACSR should include high-level location information, sponsoring organization, classification level, and unclassified indicators of available capacity. The registry should enable MILDEPs and contracting officers to identify existing, underutilized accredited facilities before approving new construction or major expansions. FSOs should be responsible for maintaining current capacity data as part of their normal duties. The registry should be hosted on JWICS with role-based access controls to protect operational security.

Enterprise DOW SCIFs. In the longer term, the Department should establish a formal additional category of accredited classified facilities designated as Enterprise DOW SCIFs, intended to complement, not replace, existing MILDEP-owned SCIFs. Enterprise DOW SCIFs would be accredited and governed at the Department level to support multiple missions across multiple MILDEPs where shared access and co-use are operationally advantageous. MILDEP-owned and mission-specific SCIFs would remain an essential part of the classified infrastructure. Enterprise DOW SCIFs would be used selectively for cross-MILDEP programs, multi-sponsor efforts, CIaaS models, and environments where reciprocity and shared access are critical to mission execution.



Implementing this additional category would require updates to DODM 5101.21 and related policy to clarify enterprise ownership, inspection authority, reciprocity expectations, and risk accountability. Enterprise DOW SCIF standards should meet or exceed ICD 705 requirements. Facility-level accountability would reside with the designated enterprise authority, while MILDEPs would retain responsibility for activities conducted within the space. This model would reduce duplication, increase utilization, and support a more agile and resilient industrial base without disrupting MILDEP mission ownership.

Impact for Warfighter

Effective enforcement of DOW SCIF reciprocity enables faster use of existing accredited facilities, allowing classified development, integration, and sustainment activities to proceed without unnecessary administrative delays. When accredited DOW SCIFs are accepted consistently across MILDEPs and regions, programs can plan facility use with confidence and avoid redundant revalidations that interrupt mission execution.

Operationally, reliable reciprocity supports smoother multi-program and cross-MILDEP integration by enabling the DIB to collaborate in shared classified environments with timely access to required systems and data. Strategically, improved utilization of existing DOW SCIF capacity reduces duplication, lowers infrastructure costs, and increases agility across the DIB. These outcomes align with broader Administration[104] and GSA[105] objectives to optimize the federal footprint and deliver greater return-on-investment for both the warfighter and the taxpayer.

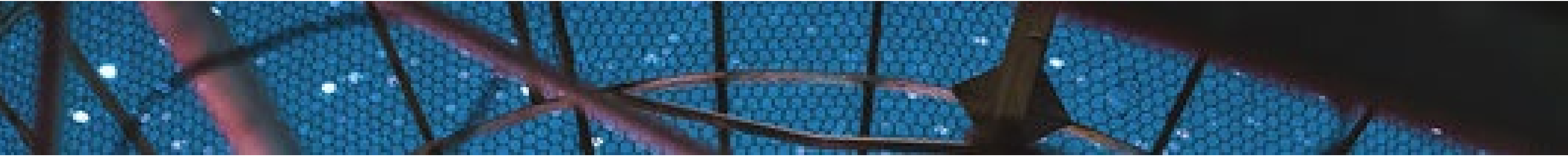
37) Underuse of Co-Use Agreements Forces Redundancy and Underutilization

Challenge

Despite clear authorization for SCIF co-use under existing policy, the DOW underutilizes co-use arrangements, leading to duplicated facility build-outs, increased costs, and inefficient use of limited classified infrastructure. Co-use agreements allow multiple programs or contractors to share existing accredited SCIFs when their requirements align. However, most interviewees revealed that these agreements remain uncommon due to cultural hesitation, lack of standardized processes, and misperceptions about risk and authority. The FAST Study questionnaire data show that only 67% of the DIB reported active SCIF co-use agreements and 77% reported active SAPF co-use, but approval timelines (including reports up to 52 weeks) still make co-use operationally unreliable. In practice, co-use agreements should enable rapid collaboration to share classified information between two MILDEPs in a classified facility. However, instead of cost-effectively sharing an existing SCIF across multiple programs with comparable requirements, MILDEPs build separate facilities even in the same building or business infrastructure. In some buildings, multiple nearly identical SCIFs are sponsored by different MILDEPs, while nearby programs lack access

[104] The White House (2025). *Implementation of the Utilizing Space Efficiently and Improving Technologies Act.* Source: https://www.whitehouse.gov/wp-content/uploads/2025/02/M-25-25-Implementation-of-the-Utilizing-Space-Efficiently-and-Improving-Technologies-Act.pdf

[105] GSA (2025). *Occupancy and Utilization Reporting Guidelines*. Source: https://www.gsa.gov/real-estate/real-estate-services/for-federal-customers/use-it-act-and-occupancy-data/reporting-guidelines

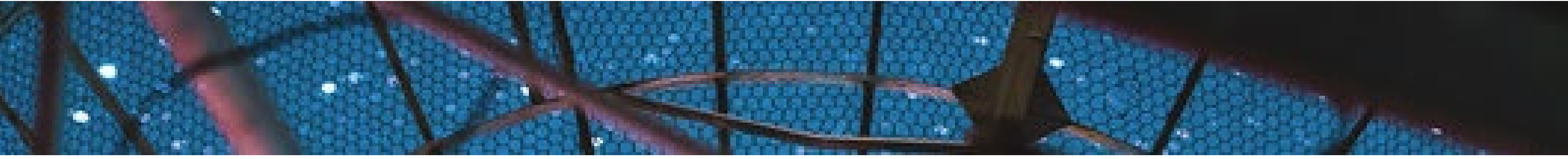


to any of them. This underuse of co-use creates redundancy, increases costs, and artificially constrains capacity. One interviewee noted, *“Everyone is afraid to let another program into their SCIF, even though policy allows it.”* Others explained that they lacked templates or guidance for structuring co-use agreements, leaving them uncertain about roles, responsibilities, and oversight implications.

> *“Co-use is allowed on paper, but the approval timeline makes it unusable.”*
> – Industry interviewee

Multiple interviewees indicated that DCSA can take up to a year to approve co-use agreements, even when a MILDEP is willing to accept the risk. The FAST Study q*uestionnaire data showed the same pattern, where four DIB* companies reported SCIF co-use approvals average of 10 weeks (median 10) and seven DIB companies reported SAPF co-use approvals average of 16.6 weeks (median 16), with longest reported approvals reaching 52 weeks for both SCIF and SAPF. In one case, an interviewee described that prolonged uncertainty and delays associated with obtaining a co-use agreement led the program to pursue construction of a new server room, ventilation system, and power distribution system within the same building, rather than relying on an existing accredited space. The interviewee did not indicate that new construction was formally required by policy. Instead, the absence of timely approval made reuse of the existing facility operationally infeasible within program timelines.

Government sponsors reportedly most often hesitated to approve co-use, fearing that shared occupancy may complicate accreditation, introduce ambiguous ownership, or require additional monitoring. In practice, the requirement to negotiate co-use agreements has become a deterrent in its own right. Industry (and likely government) perceives the co-use process as slow, uncertain, and risky, so they conclude that building or controlling separate SCIFs is safer than navigating a complex approval process to use space that already exists. However, these concerns frequently stem from misunderstanding rather than actual policy barriers. The result is predictable: multiple DOW programs in the same geographic area construct separate SCIFs, sometimes even in the same building, each carrying full cost and approval burdens which in turn increases cost to the government and companies. Subcontractors, especially small and medium sized companies, are most affected because they lack capital to build or lease dedicated SCIFs and rely heavily on shared spaces. Co-use challenges create a waste of time and resources. The USG is willing to grant personnel clearances and authorize them to handle highly sensitive information, yet often refuses to let those same cleared individuals sit together in an existing accredited space for a classified meeting or working session. Several interviewees stated that the DOW behaves as if the MILDEPs are separate enterprises guarding their own space, rather than parts of a single DOW pursuing the same mission to support the warfighter.



Company Experience: A company supporting a SAP program attempted to establish a SCIF co-use agreement after the SAP customer offered access to an existing accredited space within the same commercial building. Despite the SAP customer agreeing to provide DCSA access and even offering to document protections in writing, DCSA rejected the arrangement, citing regulatory requirements rather than specific vulnerabilities or risks. The decision was reportedly tied to DCSA's control over a single entry point (“a door”) to the facility, which was deemed insufficient for co-use.

The company noted that the accredited space already exceeded collateral requirements, including TEMPEST shielding, and that the SAP customer had committed to sharing the space. However, DCSA maintained that a separate facility was necessary, leading to the construction of a new SCIF within the same building. This process introduced significant delays and additional costs, with no apparent identified security improvement. The company described having “everything” in place: an accredited space, shielding, and even written agreements. However, DCSA still denied the request, and the company had to stop everything and build a new facility. The interviewee highlighted that the decision was framed as regulatory compliance rather than risk-based, forcing the program to duplicate efforts and restart facility timelines without addressing any tangible security concerns. “It was mindboggling.”

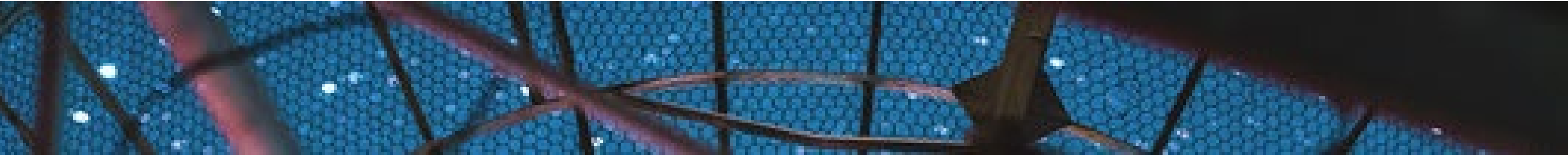
Recommended Government Action

DOW should issue guidance establishing co-use of existing accredited classified space as the default operating model, explicitly shifting co-use from an exception to the standard expectation. The need for bespoke co-use agreements should be eliminated through standardized, pre-approved co-use constructs that allow MILDEPs and DIB companies to operate in existing DOW SCIFs through a streamlined administrative process. To enforce this shift, programs proposing construction or exclusive control of new classified facilities should be required to document why existing accredited space cannot be used. This justification should be reviewed as part of facility approval, acquisition planning, or program protection review processes, and deviations from co-use should be approved only for clearly defined high-risk, mission-specific, or special-access cases.

DCSA, in coordination with OUSW(I&S), should publish uniform criteria for acceptable co-use arrangements and provide advisory support to programs evaluating shared infrastructure options. OUSW(I&S) should track and report co-use utilization, approval timelines, and instances where new construction is approved instead of reuse, enabling DOW senior leaders to identify patterns of noncompliance and address cultural or organizational barriers to shared use.

Impact for Warfighter

When classified workspaces cannot be reliably shared, innovation slows at the speed of infrastructure rather than mission need. Cleared engineers and analysts supporting different MILDEPs are prevented from working side-by-side, limiting informal collaboration, rapid problem-solving, and cross-program integration that often produce the most meaningful advances



in warfighter capabilities. As one large DIB contractor noted during interviews, the absence of shared classified space directly constrained their ability to convene SMEs across programs to explore new operational concepts and design tradeoffs in real-time.

Operationally, underused co-use forces warfighters to wait while redundant facilities are designed, built, and accredited, even when accredited seats sit empty nearby. This constrains surge capacity, delays integration and testing, and slows response to emerging threats. Strategically, continued reliance on isolated, single-program SCIFs increases cost, fragments the industrial base, and diverts resources away from accelerating capability delivery. Treating classified space as a shared enterprise asset rather than a program-owned entitlement enables faster collaboration, faster iteration, and faster advantage for the warfighter.

38) Mandatory Replacement of "Black-Label" Security Containers Imposes High Cost for Perceived Marginal Security Benefit

Challenge

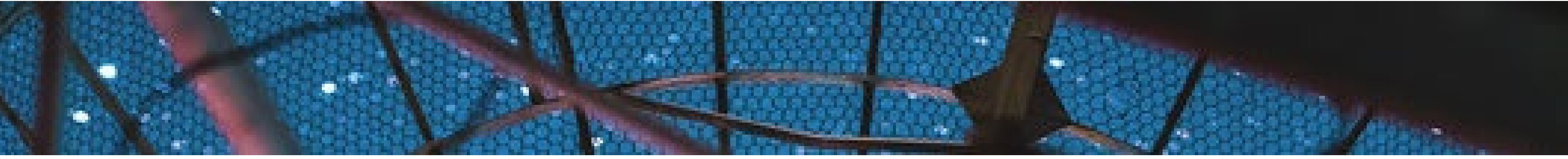
The DIB faces significant cost and operational disruption resulting from the General Services Administration (GSA) mandate to phase out and replace all approved security containers and vault doors bearing "black labels" between October 2024 and October 2028. This requirement applies broadly, including to containers that remain fully functional and are already deployed within accredited secure facilities, such as SCIFs, where multiple layers of physical and procedural security are in place.

Industry feedback indicates that the mandated replacement of black-label containers will require the DIB to incur hundreds of millions of dollars in costs over the implementation period. These costs are borne without a clearly articulated threat basis or evidence of adversary compromise associated with black-label containers shared with the DIB, many of which have been in secure use for decades. As a result, companies are required to divert limited security investment resources away from higher-value risk mitigation activities to comply with a prescriptive equipment replacement mandate.

The current approach treats all black-label containers uniformly, regardless of their condition, usage context, or the presence of compensating security measures. This lack of a risk-based or condition-based assessment framework creates unnecessary burden for both industry and government oversight organizations, while providing only marginal incremental improvement in overall safeguarding posture. From an operational perspective, the mandate also introduces planning uncertainty and execution risk, particularly for small and medium sized companies that lack the capital flexibility to absorb large, unplanned equipment replacement costs. These impacts ultimately flow through to program pricing, schedules, and delivery timelines.

Recommended Government Action

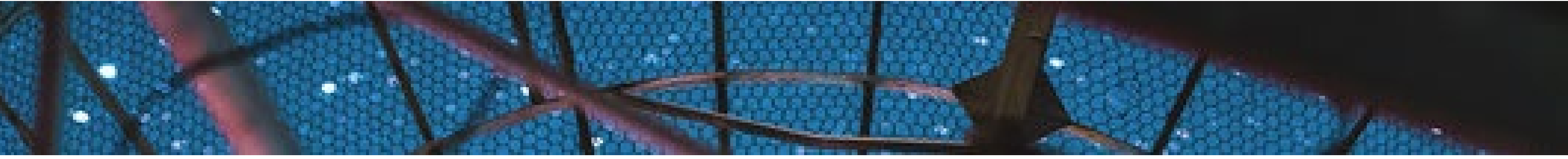
The GSA in coordination with OUSW(I&S) and DCSA, should adopt a risk-based approach to the black-label security container phase-out that allows continued use where containers are demonstrably functional and deployed within environments employing security-in-depth



measures. Where government determines that replacement is still necessary due to substantiated risk, it should provide clear threat context and implementation rationale to enable the DIB to prioritize investments and plan replacements in a manner that aligns with mission risk and operational realities. This may include condition-based assessments, extended timelines, or targeted exceptions rather than blanket replacement requirements.

Impact for Warfighter

Adopting a risk-based approach to security container replacement preserves limited security investment resources for higher-impact safeguards while maintaining appropriate protection of classified information. Reducing unnecessary cost burdens on the DIB supports program affordability, stability, and execution predictability. For the warfighter, this translates into fewer program disruptions, lower downstream cost impacts, and improved focus on security measures that meaningfully enhance protection of mission-critical information and capabilities.



Classified Infrastructure-as-a-Service (CIaaS)

As the FAST Study progressed, it became clear that commercial CIaaS offerings are emerging to fill perceived gaps in access to classified facilities. CIaaS providers offer fully managed, shared, accredited classified facilities with associated IT networks (e.g., SIPRNet, JWICS). DIB companies with FCLs can rent or lease the infrastructure on a short, mid-term-, or long-term basis with different payment options depending on the CIaaS provider. To understand how CIaaS might affect facility access and competition, the FAST Study explicitly asked DIB interviewees about their interest and experience with CIaaS models.

Based on FAST Study analysis, the DOW should continue to expand models for CIaaS to support small business participation and competitiveness, reducing dependency on large prime contractors. These DOW efforts with CIaaS models should build upon and complement prior government efforts, pilot programs, and Congressionally-mandated initiatives.[106] By expanding CIaaS availability, the Department can enable small businesses and NDCs with more rapid and consistent access to classified facilities and systems without requiring them to build and maintain their own. If implemented effectively, CIaaS will lower cost and expertise barriers to entry for small businesses and NDCs, broaden competition for classified work, and reduce structural dependence on prime contractors controlling most accredited facilities.

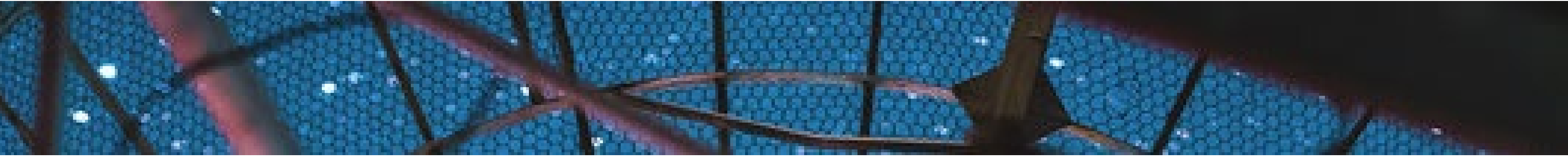
Larger DIB companies reported evaluating CIaaS offerings but still see primary value in their own accredited facilities, which they control and have already amortized over long-term programs. CIaaS was viewed mainly as a tool, for example to cover temporary loss of an existing classified facility, support short-term surge, or stand up capability in a geographic area where the company does not already have SCIF capacity.

OUSW(I&S) should use CIaaS models to identify and implement policy, accreditation, and implementation changes needed to enable routine, repeatable use of classified facilities and systems across the DIB. The DOW should direct DCSA and other accrediting organizations to move beyond ad-hoc exceptions, and develop practical, scalable, and timely processes for sponsorship, authorization, and co-use of CIaaS facilities.

DOW should also monitor and enforce guardrails on CIaaS provider business practices to ensure the model remains accessible to small businesses and NDCs. In at least one industry interview, a CIaaS provider reportedly required them to sign a contract and pay nonrefundable fees simply to “lock in” space for a proposal; there was no refund from the provider if the company did not win the contract. Though the study could not verify the case, if this business practice became the norm it would cause significant problems. For small companies operating on narrow margins and facing unpredictable win rates, such “pay-to-bid” requirements would make CIaaS unaffordable.

DOW facility accreditation and information system accreditation processes should prohibit CIaaS providers from charging nonrefundable, pre-award reservation fees solely to be named in proposals as providers of facilities. Instead, the CIaaS providers could make pre-award reservation charges fully refundable if no award is made. These protections are essential to prevent CIaaS from becoming a de facto “pay-to-compete” barrier and to ensure it functions as an on-ramp rather than a financial hazard for smaller companies. Second, DOW should direct contracting activities to specify such nonrefundable pre-award reservation fees are unallowable costs on DOW contracts and include solicitation language stating that as a condition of the accreditation, CIaaS providers may not charge nonrefundable pre-award facility fees.

[106] U.S. Congress (2024). *Servicemember Quality of Life Improvement and National Defense Authorization Act for Fiscal Year 2025.* Source: https://www.congress.gov/bill/118th-congress/house-bill/5009/text



Classified Systems and Networks

39) SIPRNet Provisioning Is Slow, Opaque, Regionally Inconsistent, and Constrained by Outdated Filtering Models

Challenge

SIPRNet provisioning was identified across interviews as one of the most persistent bottlenecks in classified work. Based on interviews, SIPRNet provisioning frequently takes two years from start to finish due to fragmented workflows, inconsistent expectations across Defense Information Systems Agency (DISA), DCSA, and MILDEP CIOs, and reliance on outdated "filtered access" models that restrict required services and drive personnel to unsecure workarounds.

Layered oversight among DISA, DCSA, and MILDEP CIO organizations, each with its own review standards, contributes to these delays. Handoffs between organizations often lack transparency, and programs have no reliable method to track progress or escalate stalled requests. Evidence expectations differ across regions, forcing contractors to recreate packages depending on which office reviews them. After all those hours of effort, the contract requiring and sponsoring SIPRNet access often ends before the DIB gets through the current process.

The reliance on static, manually defined access filtering further complicates provisioning. As part of Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6211.02D,[107] there is a requirement for DIB companies' SIPRNet access to be "filtered and limited to only those data and services required to support the DOD-approved mission." In practice, filters rarely reflect actual mission needs and frequently block required services. Personnel attempting to access SIPRNet-hosted tools or data often find that necessary ports or services are not permitted through the filter. This results in mission delays and, in some cases, unsecure workarounds. Multiple interviewees described scenarios in which personnel physically transferred classified media because filtering rules prevented access to accredited SIPRNet services. This practice significantly increases handling risk and contradicts the intent of CJCSI 6211.02D.

> *"SIPR provisioning commonly takes a year or more and that's the best-case scenario."*
> – Industry interviewee

Recommended Government Action

DOW CIO and OUSW(I&S) should develop an enterprise SIPRNet provisioning portal that unifies submission, tracking, adjudication, and escalation across DISA, DCSA, and MILDEPs. A Department-wide SLA, targeted at no more than 180 days, should define milestones, responsibilities, and resolution timeframes. Filtering should be modernized by DISA to rely on identity and data-layer enforcement rather than static network restrictions, allowing mission-required services without compromising security. Additionally, DCSA should standardize

[107] Chairman of the Joint Chiefs of Staff (2012). *Chairman of the Joint Chiefs of Staff Instruction 6211.02D: Defense Information Systems Network (DISN) Responsibilities.* Source: https://www.jcs.mil/Portals/36/Documents/Library/Instructions/6211_02a.pdf

evidence templates and review criteria across regions, ensuring consistent expectations regardless of geographic office.

Impact for Warfighter

Streamlined, transparent SIPRNet provisioning enables faster classified analysis, targeting cycles, and operational planning by ensuring timely access to required mission systems and data. When provisioning timelines are predictable and workflows are visible, programs can plan integration and testing activities with confidence, accelerating readiness and reducing delays in mission execution.

Operationally, modernized provisioning and filtering models allow personnel to access mission-required services securely, reducing reliance on manual workarounds and improving the reliability of classified workflows. Strategically, consistent and timely SIPRNet access supports modernization efforts, strengthens industry participation in classified programs, and reinforces secure handling practices. The result is improved operational tempo, reduced risk, and greater confidence that classified capabilities are available when and where the warfighter needs them.

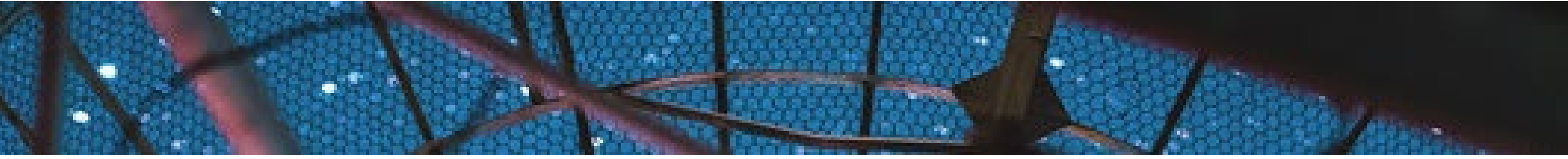
40) Classified Cloud Adoption Is Impeded by Redundant Information Owner Approval Requirements

Challenge

The DIB faces significant delays and uncertainty in adopting classified cloud environments due to requirements to obtain individual information owner approval prior to onboarding programs, even when those cloud environments have already been fully accredited through established government processes. Under current practice, contractors are often required to seek information owner approval pursuant to DFARS 252.239-7009 and 252.239-7010 before using a classified cloud environment to perform contract work. This requirement is applied even where the classified cloud environment has already undergone a robust accreditation process, including authorization by DCSA and the Defense Information Systems Agency (DISA). This additional approval step introduces schedule risk, increase costs, and discourages migration away from legacy classified systems, despite the availability of standardized classified cloud platforms. As a result, warfighter programs encounter approval timelines that can extend for months, creating uncertainty in program planning and delaying delivery.

There is no corresponding requirement for information owner approval to use non-cloud classified information systems that have already been accredited through established authorization processes. This creates inconsistent treatment between cloud and non-cloud classified environments, even though classified cloud platforms are subject to centralized, standardized, and continuously monitored security controls.

Evidence from large DIB companies collected for the fast Study indicates that these approval requirements have slowed or deferred classified cloud migrations, forcing programs to remain on older, fragmented, and more costly classified system architectures. In practice, this undermines



broader Department objectives to modernize classified computing environments, reduce system duplication, and strengthen cybersecurity posture.

Recommended Government Action

OUSW(A&S), in coordination with OUSW(I&S), should issue implementation guidance clarifying that the information owner approval requirements in DFARS 252.239-7009 and 252.239-7010 do not apply to DIB use of classified cloud environments that have already been authorized by DCSA and DISA. Where classified cloud platforms have undergone centralized accreditation and authorization, those authorizations should be treated as sufficient for safeguarding purposes, absent clearly articulated, program-specific risk factors that warrant additional review.

Impact for Warfighter

Clarifying and streamlining approval requirements for classified cloud environments enables programs to transition more quickly to standardized, secure computing platforms. Faster adoption of classified cloud reduces reliance on legacy systems, improves cybersecurity consistency, and shortens development and delivery timelines. For the warfighter, this translates into more timely access to capabilities, reduced program delays caused by administrative approvals, and improved resilience of classified systems supporting operational planning, analysis, and mission execution.

41) Metadata Is Not Preserved or Trusted Across Systems, Preventing Reliable Marking and Cross-Domain Movement

Challenge

DOW lacks a consistent, interoperable metadata framework capable of reliably preserving classification, CUI markings, dissemination controls, and provenance across systems and domains. When metadata is automatically stripped, transformed, or inconsistently applied, it becomes impossible to automate markings, enforce access controls, or enable trustworthy cross-domain transfers, forcing users back into manual processes and reintroducing human error.

Metadata is the information that describes the characteristics of data, and includes metadata that describes data contents (i.e., security labels).[108] It can be applied to specific portions of data, including sentences or words, meaning that metadata is describing characteristics of a sentence including level of classification. Metadata should be the primary mechanism for solving inconsistent marking and dissemination problems. Instead, metadata frequently fails to survive routine DOW workflows. As information moves between unclassified (e.g., NIPRNet), Secret (e.g., SIPRNet), and Top Secret (e.g., JWICS) domains; SAP, coalition networks, cloud enclaves, and CDSs, classification tags, CUI categories, dissemination instructions, and provenance markers are regularly lost or corrupted. The result is not simply "bad metadata" but a system in which metadata cannot be trusted to carry authoritative markings. Automated marking tools rely on metadata, yet MILDEPs use different schemas, different toolchains, or disable automated tagging

[108] NIST (2020). *Security and Privacy Controls for Information Systems and Organizations.* Source: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

entirely. Many CDS configurations strip metadata by default, forcing analysts to manually reconstruct classification guidance, defeating the purpose of automation and introducing substantial risk.

One industry interviewee supporting multiple MILDEPs described that *“each domain [service] implements its own flavor of metadata and marking formats.*” (The data)*“breaks the moment it crosses a boundary,”* and systems *“… require them to reapply markings manually, even when the original document contained correct metadata.”* These failures undermine consistency in higher-order functions such as access control, AI triage, document lineage, search, audit, retention, and legal discovery. One interviewee described that *“each domain [service] implements its own flavor of metadata and marking formats.”*

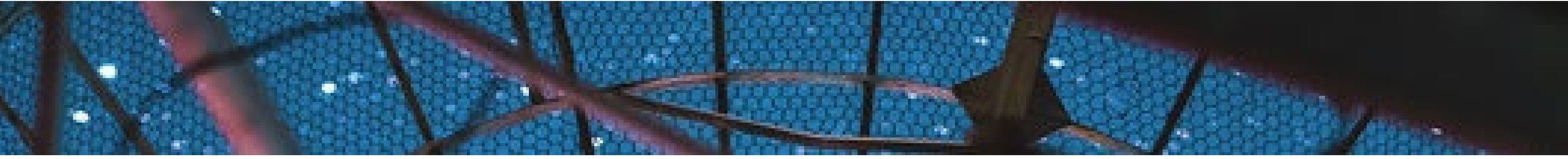
At the cutting edge of innovation, the DIB’s support to the warfighter is impacted by metadata challenges. The metadata challenges cause cross-domain transfer delays which impede mission planning and collaboration as relevant information cannot been easily transferred between unclassified NIPRNet, SIPRNet, and JWICS domains. The delays hamper the DIB’s ability to rapidly prepare and deliver effective, tailored solutions that support warfighter decision-making and operations. The metadata challenges also impede collaboration including reducing opportunities for companies to enhance impact and reduce cost by pooling and cross-pollinating current effort and prior work across MILDEPs.

The DIB currently maintains multiple, incompatible tagging schemas across MILDEPs and domains, increasing integration time and introducing unnecessary overhead cost to support the mission. Manual re-marking and metadata reconstruction also drive up the DIB’s labor hours and slows deliverables. NDCs and small businesses are hit hardest by the overhead, raising barriers to entry and squeezing margins that could otherwise be invested in other areas of security or warfighter delivery.

Unreliable metadata also introduces more errors including mishandling and unauthorized disclosure of CUI and classified information, which risks the warfighters’ battlefield advantage. Errors can also trigger audit findings and corrective actions including potential stop-work orders. Those audit findings and correction actions can affect future bidding when recorded in a company’s past performance, creating risk for the company’s future access to competitive opportunities to support the warfighter. More broadly, and not specific to the DIB, inadequate metadata infrastructure also undermines the Department’s ability to adopt AI, automate classification, manage large information ecosystems, and securely share data with allies. Metadata could solve marking inconsistencies.

Recommended Government Action

DOW CIO should produce a Controlled Security Metadata Profile (CSMP) as the authoritative, mandatory schema for all classification markings, CUI categories, dissemination rules, provenance, and automated enforcement attributes. This schema must be consistently implemented across MILDEPs and enforced across authoring tools, records systems, email and collaboration platforms, cloud enclaves, and CDSs. Cross-domain capabilities must be required to preserve, validate, and transmit metadata rather than strip or replace the metadata. Automated marking tools



must be standardized and interoperable, ensuring metadata becomes the authoritative source of truth rather than an optional or fragile layer.

Impact for Warfighter

With a mandatory, interoperable CSMP, the DIB can move mission data across domains quickly and reliably. Metadata that survives end-to-end reduces manual re-marking, integration overhead, and errors, so the DIB can deliver tailored solutions more cheaply and quickly to the warfighter. Consistent markings lower compliance risk and audit findings, keeping programs on schedule and provides the warfighter with greater assurance when integrating DIB's solutions on the battlefield. The warfighter can rely on information faster, maintaining better situational awareness and decision speed.

42) Cross-Domain Solution Rebuilds Delay Mission Execution and Produce Conflicting Approval Outcomes

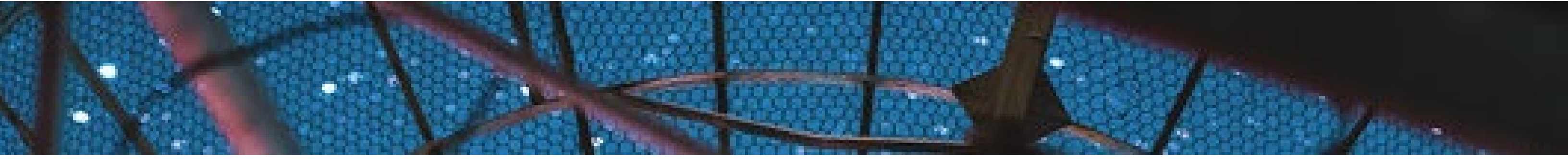
Challenge

Cross-domain data and information transfers underpin nearly every modern DOW mission set, from intelligence fusion and targeting workflows to operational command-and-control. Yet in the absence of reusable reference models, each program is effectively required to recreate guard configurations, data-flow diagrams, rule sets, and justification packages from scratch. This redundant engineering introduces avoidable cost and complexity and contributes directly to approval delays. The burden is amplified as more companies join the DIB, many of whom are required to repeat these efforts independently or, in some cases, are asked to guide MILDEPs through processes that lack standardization.

DOW lacks reusable, authoritative CDS patterns that are aligned with the Department's cross-domain governance authority, the Unified Cross-Domain Services Management Office (UCDSMO), and that programs can adopt without re-engineering. UCDSMO is the DOW's designated authority for governing and approving CDSs, but its guidance and approvals are not translated into Department-recognized reference architectures that programs and reviewers consistently accept. As a result, programs repeatedly design, document, and negotiate bespoke CDS architectures even when identical data flows and guard configurations have already been approved elsewhere.

Interviewees consistently described situations in which technically equivalent CDS architectures received materially different adjudication outcomes across MILDEPs. One industry interviewee noted, *"We built what another program built last year, but their CDS went through in weeks and ours took months, no one could explain why."* Another described *"…an identical CDS design that was approved under one component but questioned or rejected under another, forcing redesign and resubmission."* These experiences reflect not disagreement over policy, but inconsistent interpretation and risk tolerance in the absence of authoritative, reusable CDS patterns.

The challenge is further amplified by inconsistent expectations for engineering artifacts. Authorizing Officials and cross-domain reviewers routinely request different formats, levels of



detail, or evidentiary justifications when assessing comparable systems. Programs therefore rebuild diagrams, rewrite rationales, and regenerate evidence packages for each review body. This repeated rework directly contradicts the Department's goal of accelerating secure data movement and reinforces a broader theme observed across multiple FAST Study issues: the rules are not the problem, implementation is the problem.

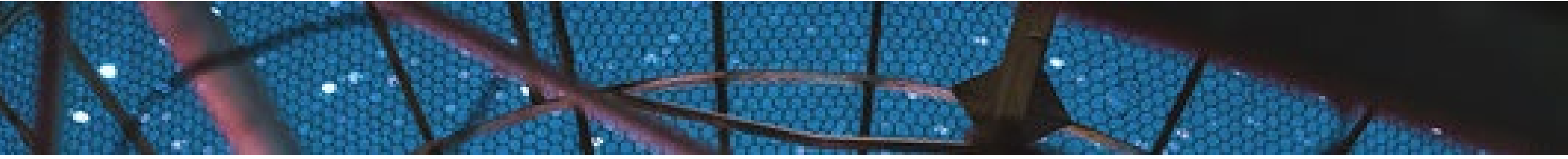
Importantly, this challenge is distinct from the challenge described in *Metadata Is Not Preserved or Trusted Across Systems, Preventing Reliable Marking and Cross-Domain Movement*. Even when metadata is intact and correctly applied, programs are still required to re-engineer and re-adjudicate identical CDS architectures because authoritative, Department-recognized patterns are not reused across MILDEPs. The cumulative result is a CDS ecosystem that is slow, inconsistent, and unnecessarily expensive. As a result, programs often experience approval timelines measured in months rather than weeks, timelines that could be significantly shortened if common, reusable, Department-developed CDS patterns were consistently applied across the enterprise. In the absence of such patterns, mission timelines slip, costs escalate, and risk decisions vary widely across the Department.

> *"We rebuild evidence more than we improve security."* – Industry interviewee

Recommended Government Action

OUSW(I&S), in coordination with the DOW CIO and the UCDSMO, should sponsor and maintain a Department-recognized library of reusable CDS patterns. These patterns should reflect commonly approved data flows, guard configurations, and risk adjudication assumptions already in use across the enterprise. Each pattern should be accompanied by standardized engineering artifacts, including reference architectures, data-flow diagrams, control mappings, and evidentiary expectations, so programs can adopt them with minimal modification unless mission-specific conditions require deviation.

UCDSMO and designated cross-domain review authorities should treat these reusable CDS patterns as baseline reference models during review and adjudication. Programs should be expected to align with the patterns to the maximum extent practical. When deviations are necessary, they should be documented explicitly and adjudicated through a defined, time-bound process focused on the delta from the approved pattern rather than a full re-evaluation of the entire architecture. MILDEPs and cross-domain review bodies should standardize evidentiary requirements for CDS approval packages based on the reusable patterns. Reviewers should evaluate submissions against a common benchmark tied to the reference models, reducing redundant rework, limiting format-driven variation, and ensuring that comparable architectures are assessed consistently across MILDEPs and regions. The ultimate solution would be the DOW developing a UCDSMO that manages a set of CDSs that all of DOW can use at an enterprise level. As each CDS carries its own data leakage risks, fewer non-enterprise DOW CDS's would reduce risk from unauthorized disclosures



Impact for Warfighter

A library of authoritative, reusable CDS patterns would dramatically reduce engineering time, standardize approval expectations, and accelerate mission data flow. Programs would be able to adopt proven architectures, reviewers would evaluate consistent designs, and warfighters would gain faster, more reliable access to the information needed to act decisively. Reducing cross-domain reengineering shortens decision timelines and improves the speed and reliability of information flow across operational boundaries. More consistent cross-domain outcomes strengthen joint and coalition interoperability, enable faster intelligence fusion and targeting, and allow scarce engineering and security resources to be focused on mission capability rather than repeated approval cycles. For the warfighter, this translates into quicker access to trusted data and greater operational tempo in contested environments.

Policy Coherence, Authoritative Sources, and Governance Alignment

43) Small Businesses and NDCs Find Complex Security Requirements Impenetrable and Costly

Challenge

Small businesses and NDCs reported significant difficulty finding, interpreting, and sequencing government security requirements across unclassified, CUI, and classified work. Guidance is fragmented across multiple sources, often written for experienced practitioners, and requires prior knowledge to understand. Small businesses and small NDCs frequently have one person responsible for security alongside other business-critical roles, increasing the likelihood of confusion, delays, unavoidable reliance on Security as a Service providers, and late discoveries about facility or system builds that affect bid decisions and performance. The absence of accessible, phase-specific, and tiered security requirements explanations increases bid uncertainty and is deterring NDCs from engaging with the DOW.

Recommended Government Action

To expand the DIB, the Department, including the DOW Defense Office of Small Business Programs (OSBP), consistent with its statutory mission and implementing regulations, should fund, advocate for, and promote specific, scalable initiatives that operationalize the translation of security requirements and socialize leading security practices with small businesses and NDCs. Pursuant to applicable law, regulation, and authoritative security policy governing the protection of government information, OSBP and cognizant security offices should sponsor and maintain repeatable leading-practices repositories and operating procedures (e.g., playbooks) that codify templates, checklists, exemplars, and decision aids. These resources should translate authoritative requirements into practical, phase-specific guidance and be distributed through existing outreach channels such as OSBP portals, industry days, and relevant consortiums.

To reduce CUI as a barrier to entry in particular, OSBP should produce and publish a Small Business Security Roadmap covering both CUI and classified work implications. The roadmap should expand standards-mapping matrices to include explicit ties to SCGs and PPPs, required facility posture, and information system implications. It should clearly distinguish bidding-phase requirements from execution-phase requirements and include decision trees, phased checklists, and links to authoritative law, regulation, and policy to guide small businesses through each security tier (e.g., Unclassified, CUI, Secret, TS, TS//SCI). The Small Business Security Roadmap and associated repositories should support role-based filtering that allows small businesses and NDCs to identify, understand, and apply legally and contractually applicable security requirements without disproportionate cost or reliance on specialized external providers. By making authoritative security expectations accessible, sequenced, and actionable, the Department can reduce bid uncertainty, lower barriers to entry, and enable broader participation in defense programs while maintaining required protection outcomes.

Initiatives similar in overall purpose to TurboFCL,[109] an online system that guides companies through completing complicated FCL forms and packages for submission, should be funded to translate government information security requirements into meaningful, plain-language execution-focused guidance. Importantly, any guidance produced should authoritatively translate and operationalize requirements for execution, focusing on explanation, sequencing, decision logic, and concrete examples rather than restating statutory, regulatory, or contractual text.

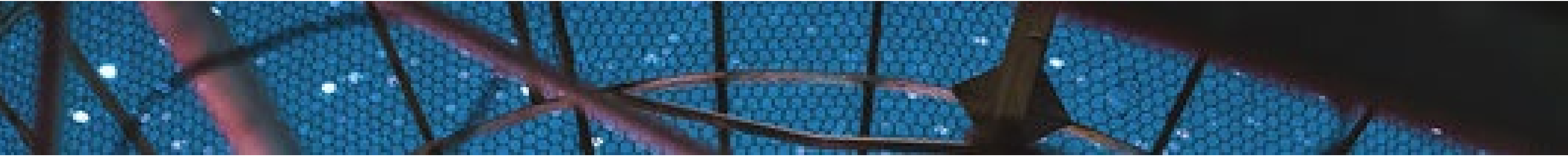
While statutes, regulations, DOW instructions, and contract clauses remain the ultimate legal authority, approved guidance should be treated as trustworthy and sufficient for compliance execution unless and until a formal conflict is identified and resolved by the issuing authority. Guidance must be governed, versioned, and traceable to its authoritative sources to ensure consistency and reduce risk of misinterpretation, bid protests, or litigation. The goal is to eliminate the need for small businesses and NDCs to independently reconcile fragmented authorities in order to perform, while preserving clear mechanisms for adjudicating discrepancies when they arise.

To further strengthen participation and competition, the Department should incentivize prime contractors to guide and assist small businesses and NDCs in understanding and implementing security requirements. Positive incentives could be tied to objective security enablement metrics such as time to first access, the percentage of small businesses and NDCs onboarded within defined timelines, and completion of CUI handling training. Primes contractors should be encouraged to offer office hours, helpdesk support, and joint readiness reviews with SMBs and the cognizant security office.

Impact for Warfighter

The recommended training and information sharing actions should result in reduced onboarding errors, lower surprise costs and delays; thus, enabling more small businesses and NDCs to enter and securely deliver their innovations to the warfighter. The result is increased, secure information processing, handling, and sharing and fewer security incidents.

[109] TurboFCL is discussed in more detail under *Recommendation 5. Complexity and Challenges in Industry Entity Clearance Eligibility Preparation.*



44) DOW Programs Cite Outdated or Superseded Policy Causing Delays or Rework

Challenge

Interviewees reported that conflicting or outdated policy references routinely trigger avoidable rework, delayed approvals, and inconsistent adjudication outcomes. As a result, RMF packages, RFP language, PPPs, and SSE artifacts routinely cite conflicting or obsolete sources, creating confusion across MILDEPs and increasing cost and rework for the DIB. Packages are returned not because security posture is inadequate, but because different reviewers rely on different versions of the same policy. This dynamic forces programs and contractors to reconcile guidance mid-review, extend authorization timelines, and resubmit documentation that is otherwise technically sound.

Programs circulate local copies of policies, rely on PDFs that have been superseded, or use archived versions that do not reflect current guidance. The absence of canonical URLs or authoritative references leads to the propagation of stale requirements, inconsistent expectations among MILDEPs, and unnecessary adjudication cycles with oversight bodies.

> *"We cannot tell which version is authoritative because program offices attach PDFs that contradict what other DOW offices tell us." – Industry interviewee*

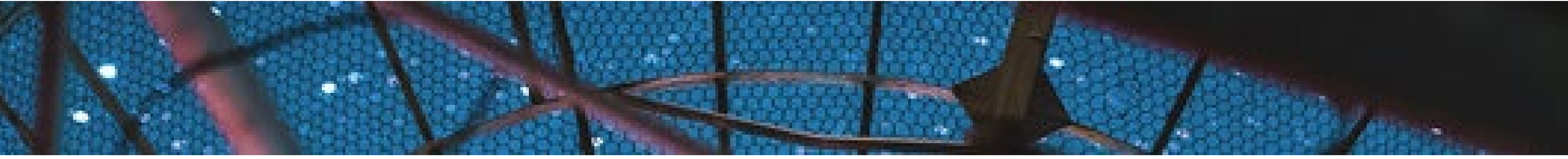
Recommended Government Action

The OUSW should create and maintain a single authoritative, version-controlled repository containing canonical URLs for all relevant security, classification, CUI, cybersecurity, RMF, and program protection policy. Programs should be required to reference this repository in all RMF, PPP, and acquisition documents, and static attachments should be treated as non-authoritative unless validated through the repository. The Department should ensure automated tools, including e-APP and RMF trackers, can validate citation currency and flag obsolete references.

Impact for Warfighter

Maintaining authoritative, current policy references accelerates approval timelines and reduces unnecessary rework, enabling faster and more predictable delivery of mission capabilities. At the tactical level, units receive systems sooner because authorization packages move through review without avoidable resubmissions driven by outdated or conflicting citations.

Operationally, consistent use of canonical policy references improves interoperability across MILDEPs and ensures more uniform protection outcomes for mission systems. Reviewers and program teams align on the same authoritative requirements, reducing friction, increasing trust in adjudication decisions, and allowing security and engineering resources to focus on mission execution rather than administrative reconciliation. The result is faster fielding, clearer expectations, and more resilient operational capability for the warfighter.



45) Overlapping Roles Between DOW CIO, OUSW(I&S), OUSW(A&S), and OUSW(R&E) Cause Divergent Instructions

Challenge

The DIB lacks clearly defined and consistently applied governance boundaries across the DOW CIO, OUSW(I&S), OUSW(A&S), and OUSW(R&E). The FAST Study interviews, focus groups, and the structure of program documentation all point to the same systemic challenge: responsibilities for classification, CUI, cybersecurity, information system requirements, and program protection are distributed across CIO, I&S, A&S, and R&E in ways that create ambiguity rather than clarity. Each office issues policy or guidance within its statutory mandate, but the boundaries between these mandates are not operationally defined, leaving programs without a clear source of truth.

This overlap is not theoretical. The DIB and government interviewees repeatedly described the practical consequences of receiving divergent instructions. For example, government interviewees found themselves *"affected by conflicting downstream instructions*" originating from different senior offices' interpretations of marking rules, system security expectations, and program protection requirements.

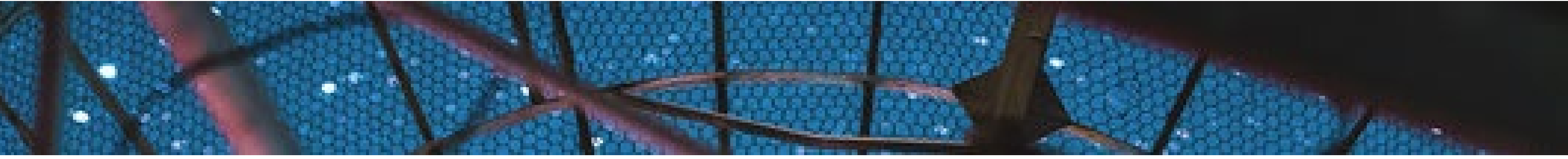
When a policy question touches classification, markings, cyber architecture, contracting requirements, and program protection simultaneously, all three offices have legitimate stakes and none have exclusive responsibility. MILDEP-level reviewers then apply their own interpretations, multiplying inconsistency.

> *"CIO says one thing applies to CUI, I&S says another, and A&S writes requirements that assume a third. We cannot tell who owns the final answer."* – Industry interviewee
>
> *"Guidance doesn't disagree because people are wrong; it disagrees because no one is empowered to decide who gets the final say."* – Industry interviewee

Recommended Government Action

OUSW should develop a formal, published Responsible/Accountable/Consulted/Informed (RACI) matrix that defines the roles, responsibilities, and decision rights of the DOW CIO, OUSW(I&S), OUSW(A&S), and OUSW(R&E) for classification, CUI, program protection, cybersecurity, and information system requirements. This matrix must be binding, operationally meaningful, and integrated into MILDEP-level policy interpretation.

The Department should also implement a time-bound adjudication mechanism that programs can invoke whenever directives from CIO, I&S, A&S, and R&E conflict. This mechanism must designate a clear final decision authority for each topic area, ensuring that governance conflicts are resolved centrally rather than pushed down to programs and contractors. Adjudicated decisions should be documented, published, and maintained in a centralized, authoritative adjudication registry accessible to programs, reviewers, and the DIB. Once issued, adjudication outcomes



should be treated as binding precedent across the Department unless formally superseded. Programs and oversight bodies should be required to apply published adjudications directly, preventing repeated escalation of identical issues, reducing inconsistent outcomes, and ensuring that governance decisions are made once and applied uniformly.

Impact for Warfighter

Clear, authoritative governance boundaries between the DOW CIO, OUSW(I&S), OUSW(A&S), and OUSW(R&E) accelerates system design, integration, and fielding by eliminating conflicting guidance and repeated rework. When programs know which senior office owns final decisions for classification, CUI, cybersecurity, and program protection, engineers can build to a stable set of requirements with confidence that approved designs will not be overturned later in the lifecycle.

At the tactical level, this clarity enables faster delivery of system updates, data access, and mission capabilities to operational units. Operationally, consistent governance improves interoperability across MILDEPs by ensuring that protection, marking, and cyber baselines are applied uniformly. Strategically, well-defined decision authority strengthens confidence in Department governance, reduces friction between oversight bodies, and ensures that critical protections are implemented consistently across mission systems. The result is faster capability delivery, more predictable execution, and stronger mission readiness for the warfighter.

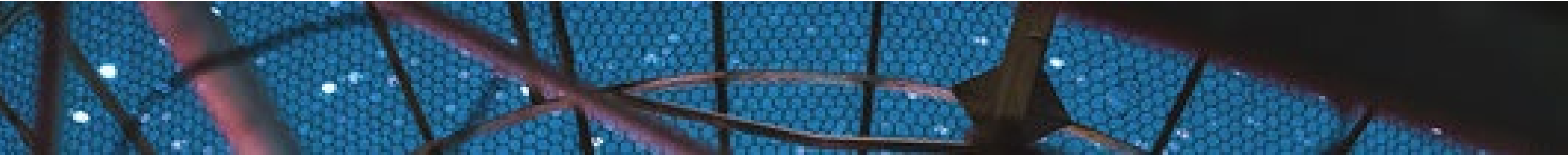
46) Regional Variation in DCSA Interpretations Burdens Industry

Challenge

Significant variation among DCSA regions in how policies are interpreted and applied results in inconsistent guidance, unpredictable facility audits, and significant disparities in DIB experience across geographic locations. During most FAST Study interviews, industry consistently reported that outcomes varied depending on which DCSA region handled their case. Some regions required additional documentation, evidence, or facility modifications that others did not. Even within the same region, expectations sometimes differed depending on the individual inspector. The lack of consistency forces the DIB to over-prepare or reinterpret requirements based on assumed regional preferences rather than written policy.

> *"We don't have a [secure facilities] problem; we have a zip-code problem."*
> – Industry interviewee
>
> *"Two facilities built from the same design received two different inspection results because different inspectors had different interpretations."* – Industry interviewee

This variability extends beyond physical facilities to classification guidance, documentation review, and follow-up inspections. As a result, contractors cannot reliably predict timelines, evidence needs, or inspection outcomes. For small businesses, these inconsistencies create



disproportionate burdens, since they lack the spare resources to absorb unexpected delays or redesign demands.

Recommended Government Action

OUSW(I&S) should reemphasize mandated uniform training for DCSA inspectors, require cross-regional calibration reviews, and implement enterprise-wide quality control mechanisms. The Department should publish anonymized metrics that reveal regional performance variation, enabling oversight and continuous improvement. Finally, DOW should implement a centralized adjudication mechanism for disputes arising from conflicting regional interpretations.

Impact for Warfighter

Consistent interpretation and application of security requirements across DCSA regions accelerates facility readiness and enables classified work to begin on predictable timelines. When inspection expectations are uniform, programs can plan execution with confidence and deliver system updates and capabilities to tactical units without avoidable delay.

Operationally, standardized regional practices improve coordination across programs and MILDEPs by ensuring that facilities built to the same requirements receive comparable treatment regardless of location. Strategically, uniform oversight strengthens trust in the facility accreditation process, improves industrial base efficiency, and allows security and engineering resources to focus on mission delivery rather than navigating regional variation. The result is faster execution, reduced friction, and more reliable support to the warfighter.

SAFEGUARDING OF CLASSIFIED AND SENSITIVE INFORMATION INDUSTRY CHALLENGES

Classified and Sensitive Information Risks

1. Programs Begin Without CPI, CTI, CUI and Fail to Establish Early, Authoritative Protection Plans
2. CUI Policy Implemented Inconsistently Across DOW
3. Lack of Standardized and Practical CUI Training Risks Mishandling

Classified Facilities

4. New Entrants and Subcontractors Face Reduced and Unpredictable Access to Classified Space
5. SCIF Accreditation Timelines Are Unreasonable
6. DOW SCIF Reciprocity Exists in Policy but Fails in Practice
7. Underuse of Co-Use Agreements Forces Redundancy and Underutilization
8. Mandatory Replacement of “Black-Label” Security Containers Imposes High Cost for Perceived Marginal Security Benefit

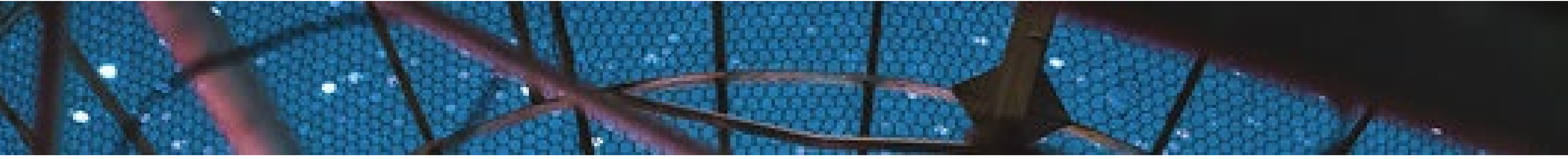
Classified Infrastructure-as-a-Service

Classified Systems and Networks

9. SIPRNet Provisioning Is Slow, Opaque, Regionally Inconsistent, and Constrained by Outdated Filtering Models
10. Classified Cloud Adoption Is Impeded by Redundant Information Owner Approval Requirements
11. Metadata Is Not Preserved or Trusted Across Systems, Preventing Reliable Marking and Cross-Domain Movement
12. Cross-Domain Solution Rebuilds Delay Mission Execution and Produce Conflicting Approval Outcomes

Policy Coherence, Authoritative Sources, and Governance Alignment

13. Small Businesses and NDCs Find Complex Security Requirements Impenetrable
14. DOW Programs Cite Outdated or Superseded Policy Causing Delays or Rework
15. Overlapping Roles Between DOW CIO, OUSW(I&S), OUSW(A&S), and OUSW(R&E) Cause Divergent Instructions



CYBERSECURITY

Cybersecurity as the Structural Constraint of the Modern NISP

The NISP remains architected for a world that no longer exists: one of bounded facilities, discrete systems, localized data, and stable technical perimeters. In that world, industrial security could be organized around physical places and individual systems. Today's missions are not.

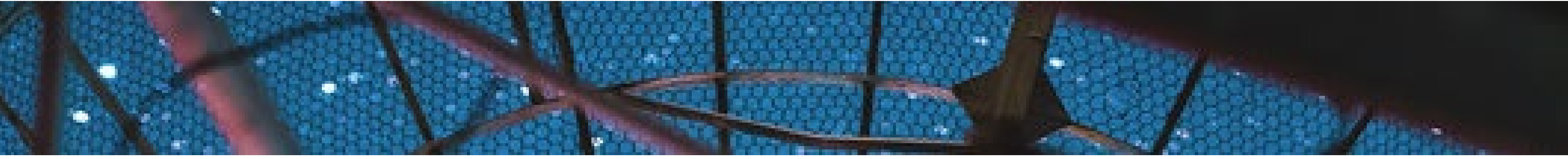
The current NISP cybersecurity model is attempting to govern a 2025 digital ecosystem with a 1995 oversight architecture. DOW operates in a fundamentally different landscape in 2025: cloud-first architectures, federated identity, Managed Service Providers (MSP) administered infrastructure, software-defined systems, Software as a Service (SaaS) ecosystems, distributed mission complexes, hybrid Information Technology/Operational Technology (IT/OT) environments, and a DIB as interconnected as it is indispensable. In this environment, cybersecurity no longer behaves like a single protection discipline but instead functions as the structural substrate upon which all other NISP obligations rest. Cybersecurity now governs identity, access, telemetry, supply chain transparency, cloud boundaries, data lifecycles, mission continuity, industry participation, and the viability of the acquisition system itself. Cybersecurity is not a co-equal pillar alongside personnel or physical security; it is the determinant of whether the DIB ecosystem can function at all.

The MITRE FAST Study's evidence—from government and industry interviews, trade association engagements, questionnaires, technical workshops, and policy analysis—demonstrates that cyber has quietly become the gating factor for DIB participation without corresponding systemic modernization of industrial security policy, governance, and oversight. Modern systems are built, deployed, and sustained through continuous development and operational pipelines in which security is embedded throughout design, integration, and runtime, not bolted on at the end.

Cyber is the structural condition under which the modern NISP must operate. Yet cybersecurity oversight is still largely executed using models inherited from physical security: static checklists, point-in-time inspections, and paper artifacts designed to attest compliance rather than validate behavior. As a result, cybersecurity-related policies, processes, and oversight models repeatedly fail to keep pace with the warfighter's missions, operational architectures, and threat tempo. This section of the MITRE FAST Study establishes cybersecurity as the structural constraint of the modern NISP. The sections that follow describe the operating environment and the empirical evidence that make that constraint unavoidable.

NISP was not Designed for the Modern Operating Environment

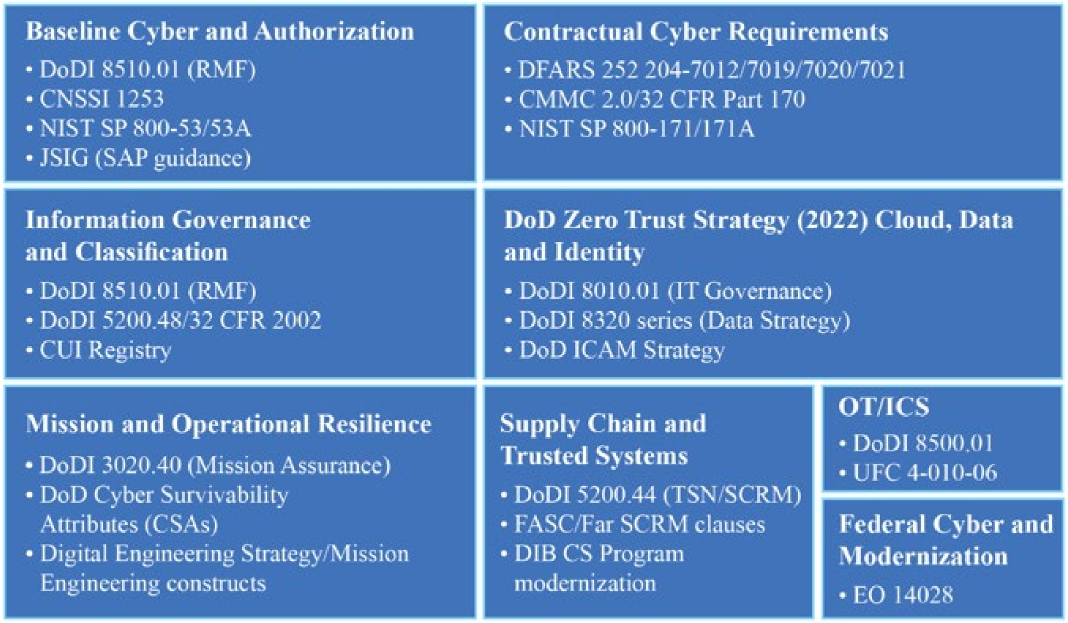
The NISP was built for a world that no longer exists. To understand why the NISP struggles with cybersecurity, it is necessary to understand the world it now inhabits. The warfighter's operating environment of 2025 bears little resemblance to the environment in which NISP authorities were conceived, nor the environment of the last major NISP update. The pace and scale of technology change, and changes in the threat landscape, have diverged sharply from the legacy oversight model that guided the NISP's development and revision.



For most small and mid-sized companies, cloud is now the default, not the exception. Enterprises run on commercial SaaS platforms, managed Microsoft 365 tenants, virtualized infrastructure, and MSP-administered environments. Identity has become the primary boundary: authentication and authorization define trust more reliably than any physical wall.

Supply chains have become ecosystems. Prime contractors, subcontractors, MSPs, and cloud/SaaS providers operate in nested, layered relationships that distribute responsibilities in ways the traditional NISP facility-centric model never anticipated. OT and mission-adjacent infrastructure have become cyber-physical hybrids: launch complexes, test ranges, Supervisory Controlled Data and Acquisition (SCADA) systems, engineering workstations, and industrial machinery that cannot be patched on traditional timelines or forced into legacy accreditation molds without breaking mission availability.

The federal environment has evolved just as dramatically. The Department now depends on a wide array of requirements and guidance for the cybersecurity and operational resilience of systems and missions, including over two dozen additional policies, directives and guidance, as well as dozens more from MILDEPs.[110] Figure 6 provides examples of the policies and guidance. Each policy and requirement is defensible within its own scope.



Baseline Cyber and Authorization
- DoDI 8510.01 (RMF)
- CNSSI 1253
- NIST SP 800-53/53A
- JSIG (SAP guidance)

Contractual Cyber Requirements
- DFARS 252 204-7012/7019/7020/7021
- CMMC 2.0/32 CFR Part 170
- NIST SP 800-171/171A

Information Governance and Classification
- DoDI 8510.01 (RMF)
- DoDI 5200.48/32 CFR 2002
- CUI Registry

DoD Zero Trust Strategy (2022) Cloud, Data and Identity
- DoDI 8010.01 (IT Governance)
- DoDI 8320 series (Data Strategy)
- DoD ICAM Strategy

Mission and Operational Resilience
- DoDI 3020.40 (Mission Assurance)
- DoD Cyber Survivability Attributes (CSAs)
- Digital Engineering Strategy/Mission Engineering constructs

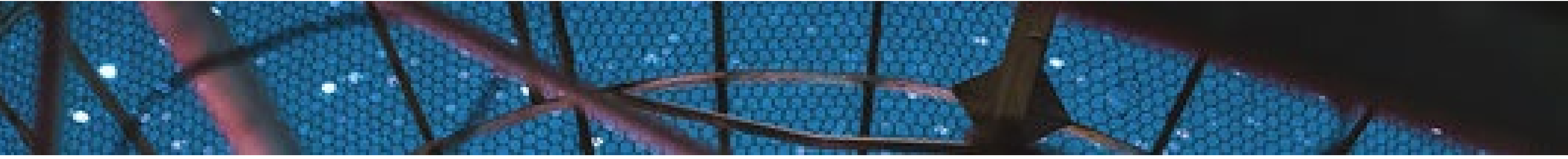
Supply Chain and Trusted Systems
- DoDI 5200.44 (TSN/SCRM)
- FASC/Far SCRM clauses
- DIB CS Program modernization

OT/ICS
- DoDI 8500.01
- UFC 4-010-06

Federal Cyber and Modernization
- EO 14028

Figure 6. Example Cybersecurity Requirements Impacting DOW Acquisition Security

[110] CUI governance (DODI 5200.48; 32 CFR 2002); DFARS 252.204-7012/7019/7020/7021; NIST SP 800-171 / 171A; Cyber Survivability Attributes and related mission resilience constructs; Mission-based resilience expectations emerging from GAO and OUSD(A&S) reviews; DODI 8510.01 (RMF); CNSSI 1253; NIST SP 800-53 / 53A; JSIG (SAP guidance); DODM 5200.01; DODI 5200.48 / 32 CFR 2002; CUI Registry; DFARS 252.204-7012/7019/7020/7021; CMMC 2.0 / 32 CFR Part 170; NIST SP 800-171 / 171A; DOD Zero Trust Strategy (2022); DISN/Cloud Computing SRG; DODI 8010.01 (IT Governance); DODI 8320 series (Data Strategy); DOD ICAM Strategy; DODI 3020.40 (Mission Assurance); DOD Cyber Survivability Attributes; Digital Engineering Strategy / Mission Engineering constructs; DODI 5200.44 (TSN/SCRM); FASC / FAR SCRM clauses; DIB CS Program modernization (32 CFR 236; DODI 8500.01; UFC 4-010-06; National Cybersecurity Strategy; and EO 14028



However, none of the frameworks were designed to fully harmonize with NISPOM, DAAPM, DAAG, or the facility-centric model embedded in today's industrial security system. The result is not a single misalignment but an accumulation of many independent policy evolutions that now intersect inside the DIB without coherence, lineage, or a clearly empowered authority to reconcile. The FAST Study did not discover these disconnects, but instead documents their full extent in the DOW. The modern cyber environment demands an oversight model capable of interpreting cloud architectures, identity boundaries, MSP responsibilities, SaaS drift, OT realities, mission continuity, telemetry, and evidence reuse, while remaining consistent across MILDEPs and defensible to mission owners. That model does not yet exist.

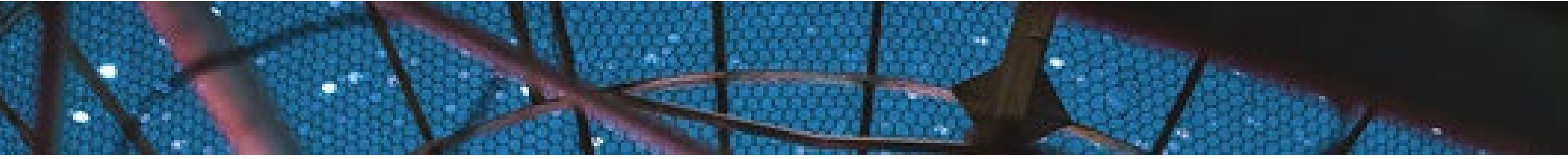
In the absence of a coherent, modern oversight model, cybersecurity Assessment and Authorization (A&A) outcomes are increasingly driven by interpretation rather than architecture. This creates inconsistent evaluation of identical systems, forces revalidation of unchanged environments, and shifts focus from mission risk to documentation details. Until the NISP is grounded in an architectural understanding of how modern systems are built and operated, cybersecurity oversight will remain reactive, inconsistent, and misaligned with operational reality.

A System Under Structural Strain

Across more than 600 qualitative data points drawn from interviews, questionnaires, technical workshops, and policy and practice reviews, the FAST Study team observed the same challenges with remarkable consistency. These were not edge cases, but recurring patterns of structural strain at nearly every interface where NISP meets modern cyber architectures.

Interviewees described being forced to regenerate nearly identical evidence packages for RMF, NISP IT authorizations, and CMMC assessments because inheritance and reciprocity are interpreted differently by each security auditor. Government assessors described cloud environments where Federal Risk and Authorization Management Program (FedRAMP) was alternately treated as authoritative or insufficient depending on MILDEP, Authorizing Official, or even individual team. MSPs described persistent difficulty aligning with NISP expectations that presume contractor-owned infrastructure. Small businesses described identity management expectations as "aspirational" and cloud approvals as "lacking transparent approval criteria." C3PAO interviewees described increasing confusion around "cloud-within-cloud" and MSP-delivered services that are built atop hyperscale cloud platforms. It is often unclear whether a company undergoing an assessment should be evaluated as a managed service operating under shared responsibility, or as a cloud service offering requiring FedRAMP or equivalent authorization. OT operators described being evaluated against control sets written for enterprise IT, not mission-critical industrial systems.

These challenges are structural indicators of a NISP that cannot align its cybersecurity obligations with the operating environment it oversees. Individually, each challenge is manageable. Taken together, they form a picture of a NISP framework no longer capable of providing predictable, mission-aligned cybersecurity outcomes across the DIB.



The core contribution of the FAST Study's cybersecurity findings is not the observation that the DIB is stressed; that observation is widely acknowledged. The FAST Study's cybersecurity contribution is the translation of this structural strain into a coherent set of 17 challenges that map where the NISP cybersecurity model fails and what must change. These represent actual points of pain that are limiting the ability of the community to support the warfighter in secure and rapidly delivering capabilities. This is not merely the conclusion of this Study, it is a widely acknowledged and shared perspective, echoed by the Department's own senior leadership past and present.

Department's Strategic Dependency on Cyber Intelligence:

"The premium on intelligence effectively informing the entire acquisition lifecycle is at an all-time high." – OUSW(I&S) Bradley Hansell confirmation testimony[111]

Mr. Hansell's statement captures the same systemic fractures surfaced across the study's cybersecurity issues, including identity and Zero Trust (ZT), cloud oversight, acquisition misalignment, and cyber threat sharing. Intelligence cannot inform acquisition when evidence, telemetry, inheritance, cloud patterns, and threat feeds remain inconsistent, slow, or one-directional.

A Department Strained by Technology and Structural Fragmentation:

"We are weighed down with legacy systems and un-optimized data… New entrants with innovative tech solutions struggle with red tape and lack of access." – DOW CIO Nominee Kirsten Davies statement to Senate Armed Services Committee[112]

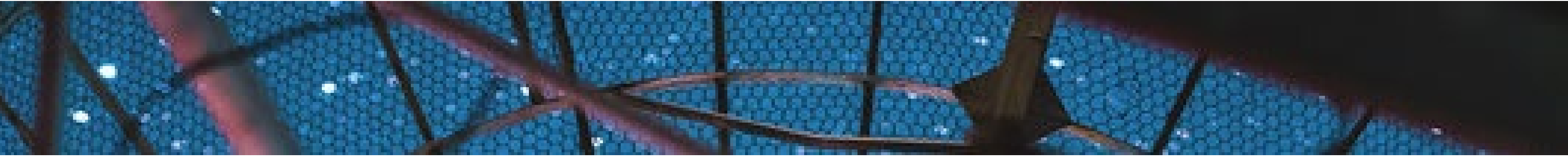
Ms. Davies emphasis that DOW must "address tech debt," "prioritize modernization," and "enable data-supremacy and decision-dominance for warfighters" aligns precisely with FAST findings.

John Sherman, former DOW CIO (2022–2024), repeatedly warned that fragmentation is itself a vulnerability. He consistently framed ZT as a foundational requirement for modern defense cybersecurity and cautioned that *"our adversaries are in our networks, exfiltrating our data,"*[113] underscoring the inadequacy of perimeter-based defenses.[1] Sherman further emphasized that Department modernization efforts are intended to "… directly aligns with the Department's cloud and software modernization efforts, which aim to drive a resilient, zero-trust-based cyber foundation in the cloud," reinforcing the need for unified architecture, identity-centric controls, and consistent baselines that FAST Study evidence shows the current NISP construct cannot reliably support.

[111] U.S. Senate (2025). *Statement of Bradley Hansell, DOW OUSW (I&S) Nominee*. Source: https://www.armed-services.senate.gov/imo/media/doc/4825fullnomtranscript.pdf

[112] U.S. Senate (2025). *Statement of Kirsten Davies, DOW CIO Nominee.* Source: https://www.armed-services.senate.gov/imo/media/doc/daives_testimony.pdf

[113] John B. Sherman, quoted in *"A Look at the DOD's Zero Trust Strategy," Resilient Cyber*, October 2022.



A Department in Urgent Need of Modernization:

"This is a cultural change, and changing culture is hard." – Acting DOW CIO Katie Arrington[114]

"We have to do better. We have to start thinking like they do… Our adversaries know our architecture." – Acting DOW CIO Katie Arrington[115]

Ms. Arrington's official establishment of the ZT Portfolio Management Office (ZT PfMO) that Mr. Sherman started signals a structural shift toward centralized governance. Their statements validate acquisition misalignment, mission survivability gaps, and AI-enabled defense tools, mirroring FAST Study's governance harmonization recommendation.

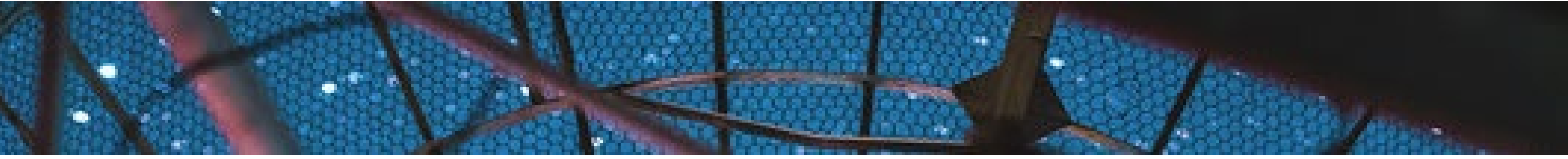
Across the Department, senior defense and cybersecurity leaders have been strikingly consistent in their diagnosis of the problem that the FAST Study now quantifies. USCYBERCOM leadership has repeatedly emphasized that effective cyber defense depends on visibility into networks, systems, and data flows, noting that threats operating outside visibility cannot be reliably defended against. DISA leadership has reinforced this shift toward identity-centric security models, aligning with the Department's broader move away from perimeter-based defenses and toward Zero Trust architectures. The SecWar has publicly underscored the operational urgency of the cyber threat, describing cyber activity as persistent, high-frequency, and growing in scale and impact. Former USCYBERCOM leadership has framed tempo itself as a decisive factor in cyberspace, emphasizing that speed, adaptability, and agility increasingly determine advantage in cyber operations. Taken together, DOW leadership is describing exactly the system the FAST Study has documented: fragmented governance, outdated architectures, duplicative oversight, unclear inheritance, and a cybersecurity model no longer aligned with real missions or modern infrastructure.

Across the FAST Study, interviewees shared similar statements:

- "We rebuild evidence more than we improve security." – Large prime contractor
- "Every reviewer treats the same cloud environment as a different system." – Government Authorizing Official
- "Zero Trust is required, but no one can tell us what it means for an MSP-run environment." – Small business CIO
- "You can't patch a rocket test stand like a laptop." – Small business OT/ICS engineer

These are not complaints; they represent structural indicators of barriers to rapid, secure acquisition for the Department. They are the visible expression of a system designed for a different

[114] Katie Arrington, remarks at the DOD Zero Trust Virtual Symposium, as reported in *Inside Cybersecurity*, April 2025.
[115] Katie Arrington, quoted in *"Pentagon CIO calls for more offensive cyber capability," DefenseScoop*, March 2025.



era, stretched beyond its intended shape. The 17 FAST Study Cybersecurity together define the transformation required for the NISP and the Department's cyber enterprise to function in today's environment.

When DOW's top cybersecurity leaders warn about fragmentation, legacy systems, inconsistent baselines, and cultural inertia, they are describing, almost point by point, the conditions the FAST Study captured in these 17 challenges. Together, these issues show that the system fails, where it fails, and why. The analysis and recommendations that follow address them as interconnected failure points in a NISP that must be rebuilt along modern architectural lines.

Across the cybersecurity issues that follow, the warfighter impact is consistent and cumulative: delayed fielding of capabilities, reduced assurance at deployment, inconsistent user experience across units and platforms, and increased sustainment burden driven by rework rather than risk. The issue-specific impacts described below trace directly to these systemic effects.

FAST Study Cybersecurity Challenges and Recommendations for the NISP

The cybersecurity challenges and recommended government actions that follow are intended to operate as an integrated set of operational changes. Together, they address systemic inconsistencies in how cybersecurity is evaluated, authorized, and sustained across the DIB, particularly for cloud-enabled, distributed, and hybrid architectures. They also reflect the reality that cybersecurity now operates at greater speed, scale, and data volume than legacy facility-centric security models were designed to manage, requiring tighter integration across industrial security disciplines. Please note that the use of the term "reviewers" in this section refers collectively to the entities responsible for cybersecurity evaluation, assessment, and authorization across the DOW and DIB, including DCSA ISRs and assessors, MILDEP Authorizing Officials and their delegated representatives, and other formally designated cyber assessment authorities. Together, these steps help to operationalize the President's Management Agenda[116] priority to defend against and persistently combat cyber enemies while modernizing how the Federal Government secures its digital infrastructure.

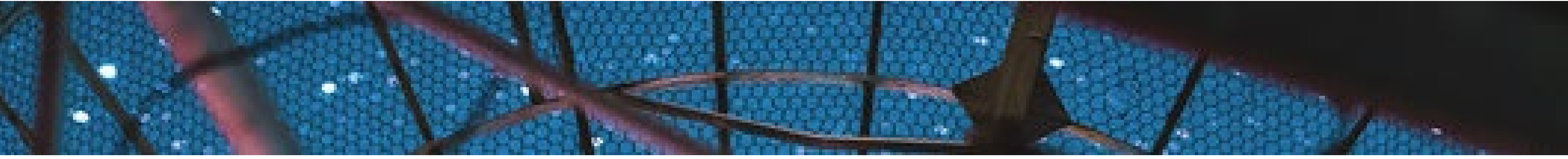
47) Misaligned System Security Plans and Inheritance Expectations Drive Rework and Reviewer Disagreement

> *"We write the same SSP five different ways because every reviewer wants something different."* – Industry interviewee

Challenge

Even when system boundaries are clearly defined, System Security Plan (SSP) expectations vary significantly by reviewer and program. The DIB is repeatedly required to rewrite identical SSP content in different formats to satisfy reviewer-specific preferences rather than risk needs.

[116] Executive Office of the President (2025). *President's Management Agenda*. Source: https://www.performance.gov/pma/



Inherited controls, particularly in cloud and MSP environments are often dismissed or expected to be restated in full, despite authoritative provider documentation.[117] This undermines the SSP's role as a stable RMF decision artifact[118] and weakens the consistency of authorization outcomes.

Recommended Government Action

The Department should mandate a standardized SSP template aligned to cloud, MSP, OT, and hybrid architectures that clearly distinguishes contractor-owned controls from inherited controls. The DOW CIO, in coordination with OUSW(I&S) to ensure consistency with NISP policy constructs, should define a standard SSP template, standardized inheritance tables, and an acceptable evidence model and should require consistent acceptance of standardized inheritance tables, control crosswalks, and references to authoritative provider documentation. DCSA and MILDEP review teams should execute this approach by standardizing review criteria and reviewer training, and by evaluating SSPs based on risk relevance and architectural accuracy rather than format or narrative depth, enforcing consistent acceptance of inherited controls.

Impact for Warfighter

Consistent SSP expectations reduce authorization friction, eliminate unnecessary rework, and shorten review cycles, enabling faster delivery of secure mission capabilities.

48) Inconsistent Cyber Evidence and Reciprocity Undermine Predictable Authorization Outcomes

> *"Same environment, same controls, but every AO [authorizing official]has their own idea of what 'good enough' means."* – Industry interviewee

Challenge

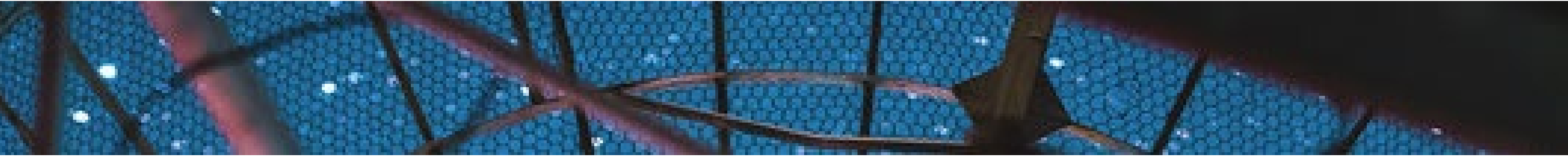
Cyber reciprocity does not function consistently in practice. Identical cloud, MSP, or hybrid architectures are repeatedly re-evaluated across MILDEPs, DCSA regions, and Authorizing Officials, even when there has been no material change in architecture or risk. There is often no standard requirement for how evidence is presented, leading to some companies submitting formalized plans and others submitting a set of screenshots. Evidence accepted in one context is rejected in another due to inconsistent interpretation of inherited controls and acceptable artifacts. This undermines enterprise risk management and prevents reuse of validated cyber evidence across the Department.[119,120] Interviewees consistently reported confusion regarding modern collaboration and shared-service platforms, particularly the distinction between endpoint environments and the underlying service management or control planes. In the absence of

[117] DOD CIO (2023). *DOD Cloud Computing Security Requirements Guide (SRG)*. Source: https://dodcio.defense.gov/Portals/0/Documents/Cloud/DOD-Cloud-Computing-SRG-v1r4.pdf

[118] DOD (2022). *DOD Instruction 8510.01: Risk Management Framework (RMF) for DOD Systems*. Source: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/851001p.pdf

[119] DOD CIO (2014). *DOD Information Assurance Reciprocity Policy*. Source: https://dodcio.defense.gov/Portals/0/Documents/DOD_IA_Reciprocity_Policy.pdf

[120] DOD CIO (2024). *Cybersecurity Reciprocity Playbook.* Source: https://dodcio.defense.gov/Portals/0/Documents/Library/(U)%202024-01-02%20DoD%20Cybersecurity%20Reciprocity%20Playbook.pdf



authoritative guidance, capabilities such as enterprise collaboration platforms and identity services are inconsistently treated as either in scope or out of scope for contractor authorization, contributing to divergent evidence expectations and inconsistent reciprocity outcomes for otherwise identical environments. While roles vary by MILDEP and authorization pathway, the FAST Study evidence indicates that inconsistent interpretation across these reviewer populations produces materially different outcomes for equivalent systems.

Recommended Government Action

Implement a mandatory, authoritative cyber evidence schema that defines acceptable artifacts for cloud-native, MSP-managed, hybrid, and on-premises systems. The DOW CIO, in coordination with OUSW(I&S) to ensure alignment with industrial security policy, should clearly define and implement enterprise-wide evidence schema and reciprocity standards, and should require consistent acceptance of inherited controls supported by validated provider attestations and enterprise authorizations. Component Authorizing Officials and DCSA regions should execute and enforce these standards by applying consistent acceptance criteria, reusing validated inherited controls, and aligning reciprocity decisions to continuous monitoring outcomes[121] rather than static documentation revalidation.

Impact for Warfighter

Effective reciprocity reduces authorization churn, shortens delivery timelines, and ensures warfighters receive secure systems faster by focusing oversight on real risk rather than repetitive documentation.

49) Conflicting RMF Interpretations Create Excessive Documentation with Limited Security Value

> *"We spend more time writing about the system than securing it."* – Industry interviewee

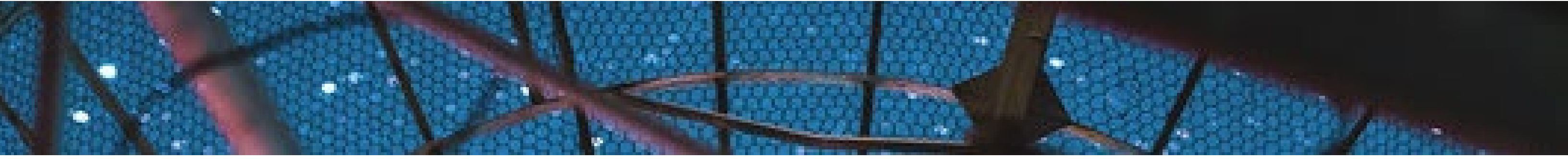
Challenge

The Risk Management Framework (RMF) provides a process that integrates security, privacy, and cyber supply chain risk management activities into the system development life cycle.[122] The RMF requires companies implement the controls in the security and privacy plans, and also document for the system and for the company a baseline configuration including specific details of the control implementation.[123] RMF documentation expectations vary widely across reviewers, resulting in expansive and inconsistent demands that are often disconnected from actual risk. The DIB is required to generate different artifacts, narratives, and evidence packages for identical systems depending on the RMF path or reviewing authority, even when architectures and controls are

[121] NIST (2011). *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*. NIST SP 800-137. Source:https://csrc.nist.gov/publications/detail/sp/800-137/final

[122] NIST (2025). *Risk Management Framework (RMF).* Source: https://csrc.nist.gov/Projects/risk-management/about-rmf

[123] NIST (2018). *NIST SP 800-53. Risk Management Framework for Information Systems and Organizations A System Life Cycle Approach for Security and Privacy.* Source: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf



unchanged. Some 47% of FAST Study questionnaire respondents reported differences in tailoring decisions by authorization path, 47% reported differences in the A&A package required, and 42% reported unclear roles and responsibilities across paths, indicating that RMF variance is driven more by pathway interpretation than system risk. This interpretive drift diverts cybersecurity personnel from continuous monitoring,[124] detection, and response activities and undermines RMF's role as a risk management framework,[125] rather than a documentation exercise.

Recommended Government Action

The DOW CIO, in coordination with OUSW(A&S) to prevent documentation growth through acquisition pathways and contract language, should define an authoritative minimum RMF documentation standard and define clear limits on expansion beyond it; ensuring that reviews emphasize risk relevance, architecture, inheritance, and continuous monitoring outcomes rather than stylistic or narrative depth. Component Authorizing Officials and DCSA review teams should execute this approach by reinforcing RMF as a decision framework grounded in risk signals, enforcing "risk relevance" review standards, and curbing pathway-by-pathway interpretive drift through consistent oversight and reviewer training.

Impact for Warfighter

Reducing unnecessary documentation burden allows cybersecurity resources to be applied to active risk management rather than administrative rework, accelerating authorization timelines and improving operational readiness.

50) Unclear Shared Responsibility Models Leave Critical Cyber Controls Unowned

> *"Half the findings we get are things the provider owns, not us."* – Industry interviewee
>
> *"We are asked for proof of things we cannot see and do not control."* – Industry interviewee

Challenge

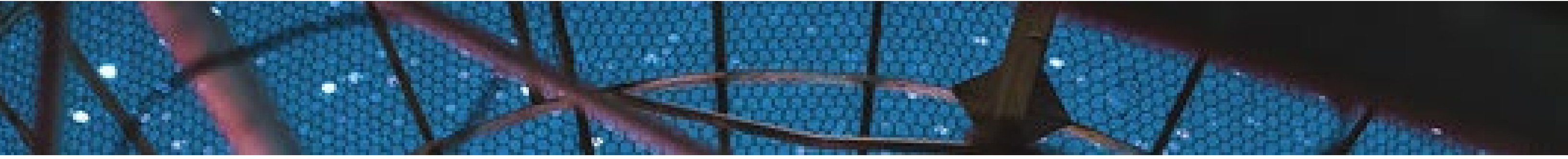
Oversight bodies frequently hold the DIB accountable for controls owned and operated by cloud service providers or MSPs, rejecting authoritative provider evidence[126] and requiring redundant contractor-generated artifacts. This reflects a persistent misunderstanding of shared responsibility models, particularly around identity enforcement, access control, monitoring, and configuration ownership.[127] Identical architectures receive inconsistent evaluations across reviewers and regions.

[124] NIST (2011). *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*. NIST SP 800-137. Source: https://csrc.nist.gov/publications/detail/sp/800-137/final

[125] DOD (2022). *DOD Instruction 8510.01: Risk Management Framework (RMF) for DOD Systems*. Source: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/851001p.pdf

[126] DOD CIO (2023). *DOD Cloud Computing Security Requirements Guide (SRG)*. Source: https://dodcio.defense.gov/Portals/0/Documents/Cloud/DOD-Cloud-Computing-SRG-v1r4.pdf

[127] DOD CIO (2020). *DOD Identity, Credential, and Access Management (ICAM) Strategy*. Source: https://dodcio.defense.gov/Portals/0/Documents/Cyber/ICAM_Strategy.pdf



Recommended Government Action

The Department should publish a unified shared-responsibility model covering cloud, MSP, hybrid, and OT-adjacent environments, with authoritative inheritance matrices that explicitly define ownership of security controls, including Identity, Credential, and Access Management and access enforcement, with the DOW CIO, in coordination with OUSW(I&S) to align acceptance of provider evidence with industrial security oversight, responsible for defining and maintaining the authoritative model and inheritance matrices. Validated provider evidence should be treated as authoritative unless mission-specific risk Validated provider evidence, including authorization packages and continuous monitoring artifacts approved through DOW CIO recognized authorization processes (e.g., FedRAMP or DOW enterprise service approvals), should be treated as authoritative unless mission-specific risk justifies deviation. Component Authorizing Officials and DCSA reviewers should execute this model by standardizing reviewer training across MILDEPs and DCSA regions and by applying consistent interpretation of shared controls.

Impact for Warfighter

Clear shared-responsibility expectations enable faster adoption of secure cloud-enabled capabilities and reduce authorization delays driven by architectural misunderstandings.

51) Cyber Reciprocity Failures Force Re-authorization of Identical Architectures

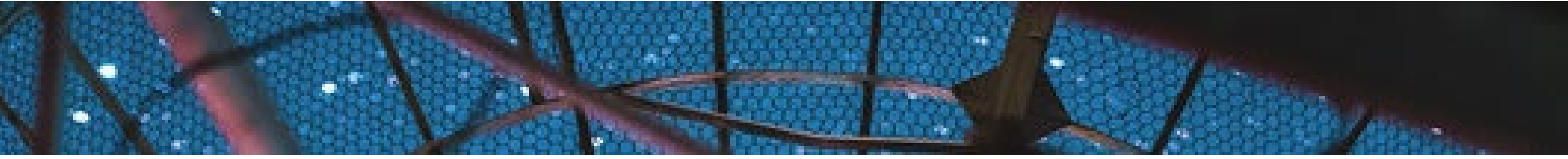
> *"Even within DCSA, regions have their own interpretations."* – Industry interviewee

Challenge

Cyber reciprocity does not function consistently across DCSA regions and MILDEPs. Identical systems and architectures are frequently re-evaluated, with inherited controls and evidence accepted in one context and rejected in another. Interview evidence indicates that reciprocity failures frequently arise from inconsistent interpretation of inherited controls, cloud responsibility models, and prior authorization scope across DCSA regions and MILDEPs. Assessors and reviewers often re-examine identical technical implementations due to uncertainty over boundaries, inheritance validity, or perceived differences in system context, even when no material risk change has occurred. This unpredictability erodes trust in reciprocity policies and drives repeated reauthorization cycles unrelated to changes in risk.

Recommended Government Action

The Department should enforce reciprocal acceptance of validated cyber authorizations and evidence across regions and MILDEPs through enterprise-level governance, with the DOW CIO responsible for defining the enterprise reciprocity enforcement model, criteria for revisiting prior authorization decisions, and standards for reusable evidence packages, in coordination with OUSW(I&S) to ensure NISP-wide alignment.



This enforcement model should establish a presumption of acceptance for previously validated authorizations and evidence, with clear, documented criteria defining when prior decisions may be revisited due to material risk change. Any deviation from reciprocal acceptance should require explicit justification tied to those criteria, rather than reviewer discretion or local practice. Standardized, reusable evidence packages should be treated as authoritative across programs and MILDEPs unless material risk has changed. Where disagreement arises regarding reciprocity application, an enterprise-level adjudication mechanism should be available to resolve disputes and prevent inconsistent re-evaluation of identical systems.

Component Authorizing Officials and DCSA regions should execute this approach by implementing reciprocal acceptance as the default, applying standardized reassessment triggers tied to material risk change, and documenting and escalating deviations in accordance with enterprise criteria.

Impact for Warfighter

Effective reciprocity reduces authorization churn and accelerates deployment of secure operational systems needed for mission success.

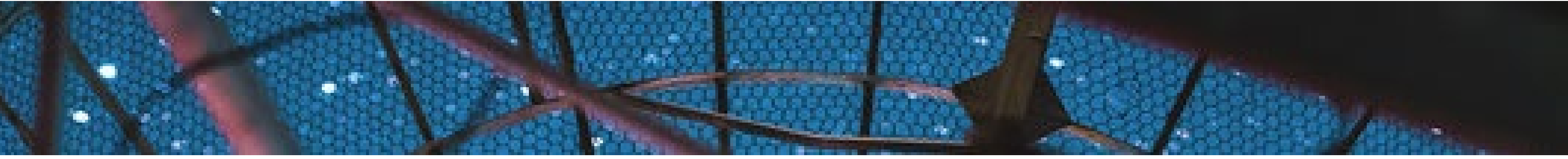
52) Inconsistent Cybersecurity Assessment Execution and Change Handling Undermine Security Outcomes, Cost, and Industrial Base Stability

> *"Two assessors can look at the same system and come away with completely different conclusions about what needs to be reassessed."* – Industry interviewee
>
> "*Because 32 CFR is silent, C3PAOs are kind of all over the place in how they're doing this, and that really scares me.*" – C3PAO interviewee

Challenge

Across the Department, cybersecurity assessment outcomes are increasingly shaped not by system architecture or control implementation, but by inconsistent assessment execution and poorly defined change handling. While policy and standards define what must be protected, insufficient guidance governs how assessments are conducted, paused, resumed, or revisited as environments evolve. As a result, identical or materially similar systems are assessed differently, routine operational changes trigger disproportionate reassessment activity, and outcomes vary based on execution approach rather than actual risk. As one C3PAO interviewee summarized, "*In 32 CFR they have this term 'significant change' to the system or boundary. What does that mean? There is no guidance.*"

These inconsistencies manifest across DCSA-led reviews, MILDEP authorization processes, and third-party certification assessments, including those performed by C3PAOs. In the absence of authoritative, scenario-based guidance, assessment bodies apply divergent interpretations

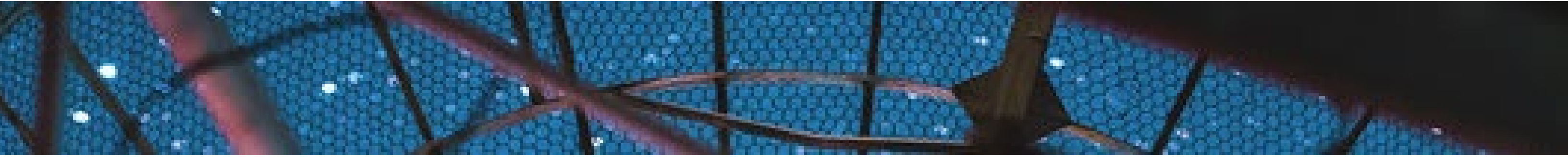


regarding what constitutes a material change, when reassessment is required, how scope should be adjusted, and what assessment methods are sufficient. The DIB are frequently unable to predict whether common activities such as adding users, expanding to additional locations, onboarding managed service providers, or incrementally modernizing infrastructure will require no action, limited review, or full reassessment. FAST Study interviewees consistently emphasized the need for *"guidance in the way of scenarios"* so companies can map routine changes to defined reassessment pathways rather than defaulting to full reassessments.

In practice, execution ambiguity also extends to how assessment resources are applied. Interview data indicates that expectations regarding assessor staffing models and the use of specialized personnel have emerged unevenly, often without clear policy direction. These expectations are applied inconsistently across assessments and can materially affect cost and accessibility, particularly for small and medium sized companies, even when system scope and risk are comparable. As one C3PAO interviewee noted, "*They're requiring three very expensive resources… two assessors… and then they require a QA,"* while also acknowledging, *"You really don't need that model in all cases."* Several C3PAOs noted that these staffing expectations do not consistently align with risk. As one explained, *"We are being told to show up with three high-cost assessors for every engagement, but that model does not map to risk. In many cases you could do it with fewer people and get the same assurance. The resource model is driving price more than the architecture is."* Interviewees also described assessor workforce availability constraints that compound execution variability and increase scheduling uncertainty. Several noted that qualified assessors can be unavailable for extended periods due to pending eligibility determinations, limiting the ability of C3PAOs and other bodies to staff assessments predictably.

Interviewees emphasized that execution variability is amplified by the absence of clearly defined roles, responsibilities, and internal execution standards within assessment teams. Expectations regarding when technical specialists are required, how assessor judgment should be documented, and how disagreements within assessment teams should be resolved are not consistently defined. As a result, assessment outcomes depend heavily on individual discretion and informal team dynamics rather than standardized assessment practice, increasing variability across assessments even when system scope and risk are comparable. Multiple assessors reported that the absence of stable, example-backed guidance is making some assessments adversarial, including instances where organizations bring legal counsel into assessment sessions because outcomes hinge on assessor interpretation rather than consistent standards.

The lack of a clear, operational construct for distinguishing material risk changes from routine updates further exacerbates these challenges. In the absence of defined limited-scope or just the delta reassessment pathways, assessors' default to full reassessments for low- or medium-impact changes, increasing cost, introducing schedule uncertainty, and discouraging modernization without delivering commensurate security benefit. Multiple assessors described just the delta reassessment as the practical middle ground: "*I ought to be able to do a delta assessment of just what's changed and charge the company a lot less money."* Several interviewees also highlighted the structural conflict this ambiguity creates for assessors themselves.



As one C3PAO explained, “*I’m not really supposed to be telling them whether it’s a significant change, it’s a conflict of interest for me, but without guidance, that’s exactly what companies are asking us to do.”*

Control-specific implementation challenges, such as those associated with NIST SP 800-171 control 3.4.7, further illustrate how ambiguous execution expectations scale poorly across diverse environments. Interviewees described organizations either over-engineering documentation to “boil the ocean” or adopting overly minimal interpretations, neither of which reliably improves security. One interviewed assessor observed that *“people get lost in this control,”* while another noted that “*the same requirement pushes large companies to build massive documentation frameworks, and then small companies are expected to somehow do the same thing.”* The result is procedural compliance and documentation churn rather than sustained, risk-informed configuration management.

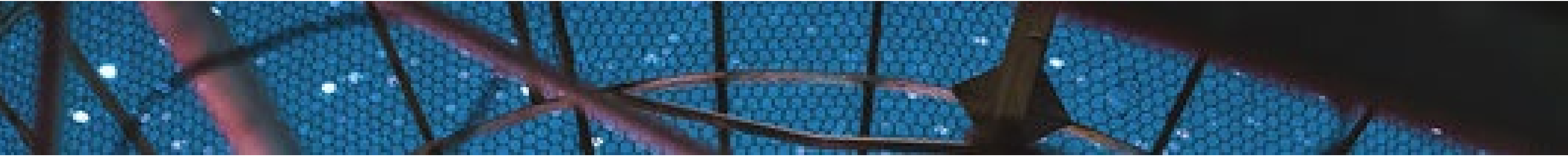
Execution variability is compounded by administrative and tooling friction. Processes for submitting, modifying, and maintaining assessment records often rely on manual intervention, specialized personnel, and repeated resubmission due to system limitations, unpredictable updates, or lack of testing environments, including enterprise A&A systems such as eMASS. As one C3PAO interviewee put it bluntly, *“eMASS is a problem for us.”* Many interviewees reported that submissions can be rejected *“for some reason that you’re not aware of,* requiring repeated rework by highly paid staff.” Others emphasized “the absence of a development or test environment,” and noting the need for *“a development environment… to test”* automation and predictable release cycles to avoid breaking assessment workflows.

> *“It takes me at least an hour to get everything into eMASS if everything is perfect, realistically it’s closer to two hours, and that’s before anything gets rejected.”* – C3PAO interviewee

Interviewees also described uncertainty around whether assessments may be paused and resumed when required capabilities are not yet operational. One assessor explained, *“If something isn’t implemented yet, I’ll stop the assessment and let them finish it within 90 days, then pick up where we left off, but I don’t know if that’s officially okay because there’s no guidance.”* The absence of clear pause-and-resume standards contributes directly to inconsistent outcomes, cost escalation, and disputes across assessment bodies.

Under mandatory certification regimes such as CMMC, these execution and change-handling ambiguities have amplified impact. Assessment outcomes directly determine contract eligibility rather than administrative timing, magnifying the consequences of inconsistent execution, unclear change thresholds, staffing variability, and tooling friction. As one interviewee warned, *“For small and medium-sized companies, getting hit with repeated full assessments is just not doable from a cost perspective.”*

One interviewee described other inconsistencies. One small industry company described completing a full Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) review of the same Government Community Cloud (GCC) High environment certified under



CMMC Level 2 earlier in the year: *"We passed CMMC Level 2 in January and then had to support a full DIBCAC of the same exact environment in October. It took twice as long, used our most expensive resources, and we had not changed a thing, but we had to start over."* The interviewee emphasized that both assessments were well-intentioned, but that *"CMMC Level 2 doesn't give you credit,"* illustrating how misaligned assessment ecosystems can drive cost and schedule independently of any underlying change in risk.

Collectively, these dynamics undermine reciprocity, reduce predictability, discourage participation, particularly among small- and medium-sized businesses, and erode confidence that assessment results reliably reflect actual cybersecurity posture. The impacts of these dynamics are important given that CMMC functions right now as a high-stakes, binary "pass or fail" examination rather than a collaborative, risk-informed process. One C3PAO characterized CMMC assessments as "*a three- or four-day pass/fail event where failure has devastating consequences,"* and noted that "*the fear of failing leads companies to over-engineer everything, rip and replace networks, buy (Federal Information Processing Standards) FIPS-validated hardware for endpoints that only ever talk to SharePoint. It is not security; it is survival."* These are rational responses to a process that concentrates contract eligibility into a single event and leaves substantial room for assessor interpretation.

Recommended Government Action

The Department should establish authoritative, enterprise-level governance for cybersecurity assessment execution and change handling, while preserving MILDEP authority for mission risk acceptance. The DOW CIO, in coordination with OUSW(I&S) to ensure alignment with industrial security and certification constructs, should define outcome-oriented standards governing how cybersecurity assessments are executed, paused, resumed, and revisited as environments evolve. These standards should include scenario-based criteria that distinguish material architectural or risk changes from routine or administrative updates, and clearly define when full reassessment, limited-scope or just the delta reassessment, or no reassessment is required.

To improve predictability and affordability, the DOW CIO and OUSW(I&S) should also clarify expectations related to assessment execution practices, including the application of assessor staffing models and the use of specialized expertise. Authoritative implementation guidance should distinguish when additional assessors or specialists are warranted based on system complexity or risk, versus when streamlined assessment approaches are appropriate. Clear execution guardrails would reduce variability driven by informal practices and improve access for small and medium-sized companies without weakening security assurance. The Department should also establish a rapid-turn authoritative guidance mechanism, such as implementation letters or scenario-based FAQs with concrete examples, to resolve recurring assessment questions in days rather than weeks during live assessments.

Component Authorizing Officials, DCSA regions, and designated assessment bodies should execute and enforce these standards consistently by applying uniform reassessment thresholds, using risk-based approaches to scope adjustment, and employing standardized expectations for documentation review, interviews, and technical validation. Expectations for on-site versus remote assessment, multi-site evaluation, and acceptable assessment pause and resumption conditions should be clarified to reduce execution variability while maintaining assurance for higher-risk environments.

To reduce administrative friction and cost amplification, the DOW CIO should improve assessment tooling and supporting infrastructure. This should include enabling automation where appropriate, establishing predictable system update and maintenance cycles, and providing testing or development environments for enterprise A&A tooling (e.g., eMASS) that allow assessors and the DIB to validate submissions and updates prior to production use. Improved tooling transparency and stability would reduce rework, minimize unnecessary reassessment triggers, and shift assessment effort toward sustained cyber risk management rather than procedural compliance.

Impact for Warfighter

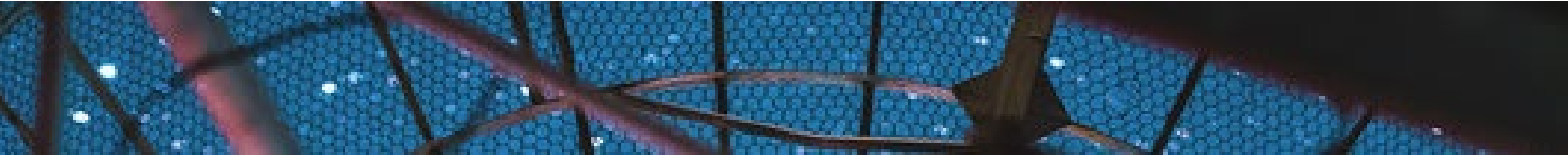
Consistent, risk-aligned cybersecurity assessment execution improves cost predictability, reduces authorization friction, and supports timely delivery of secure capabilities. Clear change-handling and reassessment standards allow programs to focus effort on meaningful risk management rather than procedural rework, enabling modernization to proceed without unnecessary delay and more affordable reassessments. By providing predictable, scalable assessment pathways while maintaining appropriate assurance for higher-risk systems, the Department strengthens BIB participation and resilience. This consistency accelerates delivery of mission-ready capabilities to the warfighter and improves confidence that assessment outcomes accurately reflect operational cybersecurity posture.

53) Variable Cloud Architecture Evaluations Block Standardized Authorization Paths

> *"Same architecture, different expectations."* – Industry interviewee
>
> *"You end up explaining the same architecture over and over, and the answer depends on who's listening."* (paraphrased from Interviews)

Challenge

Cloud architectures are evaluated inconsistently across reviewers and MILDEPs despite being built on standardized services and shared-responsibility models. Programs are often directed to "implement ZT" without authoritative, scalable baselines for identity-centric access control, segmentation, and monitoring in cloud and hybrid environments. Most FAST Study DIB respondents reported ZT implementation at scale (63–75% reporting 51–100% implementation), yet authorization outcomes still vary; indicating the gap is not adoption intent but inconsistent evaluation standards and evidence acceptance. In the absence of clear standards, reviewers apply individual interpretations, leading to inconsistent findings, repeated rework, and unpredictable authorization outcomes for unchanged cloud architectures.



The same inconsistency has led to C3PAO interviewees describing confusion around "cloud-within-cloud" and MSP-delivered services that are built atop hyperscale cloud platforms. It is often unclear whether a company undergoing an assessment should be evaluated as a managed service operating under shared responsibility, or as a cloud service offering requiring FedRAMP or equivalent authorization. Without authoritative criteria for C3PAOs making this distinction, identical service models are treated differently across MILDEPs and assessments, contributing to inconsistent inheritance decisions, duplicative oversight, and variable authorization outcomes.

Recommended Government Action

The Department should define authoritative ZTA and ICAM[128] baselines mapped to common cloud and hybrid architecture patterns, with the DOW CIO responsible for defining and maintaining the authoritative cloud, ZT, and ICAM baselines, in coordination with OUSW(A&S) to ensure these baselines are embedded early in program requirements and contractor expectations. Authorization criteria must align with DOW ZT guidance and explicitly recognize inherited cloud capabilities,[129] and reviewer training should standardize evaluation of identity-driven security controls and cloud-native evidence. Component Authorizing Officials and DCSA reviewers should execute this approach by applying standardized evaluation criteria and consistently recognizing inherited cloud capabilities across programs.

Impact for Warfighter

Clear ZT and identity expectations enable predictable implementation, reduce authorization friction, and strengthen protection of mission systems in contested environments.

54) Uniform Vulnerability Management Expectations Ignore Cloud, MSP, OT, and Legacy Constraints

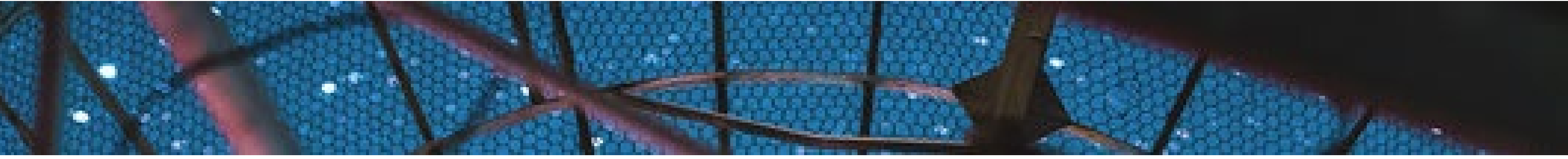
> *"Half our findings are vendor won't let you patch it."* – Industry interviewee
>
> *"We're being asked to run scanners that can't even see half the systems they want reports for."* – Industry interviewee
>
> *"You need to do something about vulnerabilities at the network level."* – Council and consortium interviewee

Challenge

Vulnerability management across the DIB is evaluated using a uniform, IT-centric model that does not reflect the operational realities of modern environments. Cloud platforms, SaaS offerings MSP-managed services, OT and industrial control systems, or legacy and vendor-controlled environments frequently operate under constraints that prevent traditional scanning, patching, or

[128] DOD CIO (2020). *DOD Identity, Credential, and Access Management (ICAM) Strategy*. Source: https://dodcio.defense.gov/Portals/0/Documents/Library/DOD-ICAM-Strategy.pdf

[129] DOD CIO (2023). *DOD Cloud Computing Security Requirements Guide (SRG)*. Source: https://dodcio.defense.gov/Portals/0/Documents/Cloud/DOD-Cloud-Computing-SRG-v1r4.pdf



remediation practices from being applied safely or directly by the contractor. FAST Study interviews consistently highlighted situations in which organizations are required to remediate vulnerabilities they do not control, apply patches that introduce unacceptable operational risk, or run scanning tools that are incompatible with mission systems. In these cases, the existence of a vulnerability or available patch is treated as equivalent to exploitable risk, even when mitigation is technically infeasible, operationally unsafe, or contractually prohibited. This results in persistent findings and long-lived POA&Ms that do not meaningfully reduce cyber risk.[130]

These outcomes are not primarily driven by inconsistent execution or assessor behavior. Interview evidence indicates that even when reviewers apply requirements consistently and in good faith, the underlying vulnerability expectations themselves are misaligned with how modern systems are built, managed, and operated. Cloud and SaaS providers often control patching and configuration baselines. OT environments prioritize availability and safety over rapid change. Legacy and vendor-managed systems may lack patch paths entirely. Applying a single vulnerability remediation model across these environments produces administrative noncompliance without commensurate security benefit.

As a result, vulnerability management effort is frequently diverted toward documenting exceptions, negotiating findings, and maintaining POA&Ms rather than reducing exploitable risk. This dynamic increases cost, extends authorization timelines, and discourages incremental modernization, while providing limited improvement in actual mission resilience. One assessor summarized this dynamic bluntly: *"We generate POA&Ms for things they literally cannot patch. The existence of a patch becomes the risk, not whether the vulnerability is exploitable in that environment."* This further reinforces that vulnerability expectations must be grounded in operational feasibility.

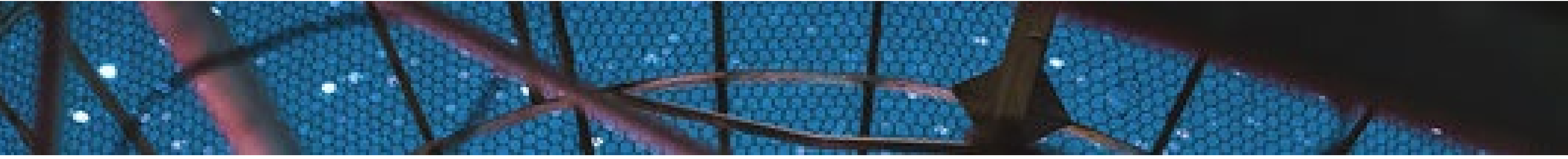
Recommended Government Action

The Department should implement an environment-aware vulnerability management framework that explicitly differentiates expectations for cloud and SaaS environments, MSP-managed infrastructure, OT and industrial control systems, and legacy or vendor-controlled systems. The DOW CIO, in coordination with OUSW(I&S) where industrial security policy interpretation drives review behavior, should define an environment-aware vulnerability management framework and specify acceptable vulnerability evidence for each environment, including clarifying when provider-managed monitoring and attestations are authoritative,[131] and distinguish between the existence of a patch and the feasibility of applying it safely.

This framework should clearly distinguish between the existence of a vulnerability or patch and the feasibility of safely applying remediation in a given operational context. It should establish standardized criteria for accepting compensating controls, architectural mitigations, and network-level protections when direct patching or scanning is impractical or unsafe. POA&Ms should be

[130] NIST (2022). *NIST SP 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations.* Source: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

[131] DOD CIO (2023). *DOD Cloud Computing Security Requirements Guide (SRG)*. Source: https://dodcio.defense.gov/Portals/0/Documents/Cloud/DOD-Cloud-Computing-SRG-v1r4.pdf



treated as a risk management mechanism of last resort rather than a default outcome for environment-constrained systems.

Component Authorizing Officials and DCSA reviewers should execute this framework by applying standardized reviewer training and evaluation criteria, assessing vulnerability risk consistently based on operational context rather than the presence or absence of traditional scanning or patching artifacts, and approving compensating controls where operational constraints limit safe patching.[132]

Impact for Warfighter

Aligning vulnerability management expectations with operational reality enables DIB programs to focus effort on exploitable risk rather than administrative closure, reducing authorization delays and accelerating delivery of mission-critical capabilities.

55) Inconsistent CUI and Sensitive Data Governance Breaks Lifecycle Protection across Modern Toolchains

> *"Give us one set of rules for how long to keep it, where we can store it, and what we can do with it. Right now, every program invents its own universe."* – Industry interviewee
>
> "*We're rebuilding the lifecycle rules for every contract because no one upstream will tell us what the lifecycle actually is."* – Industry interviewee

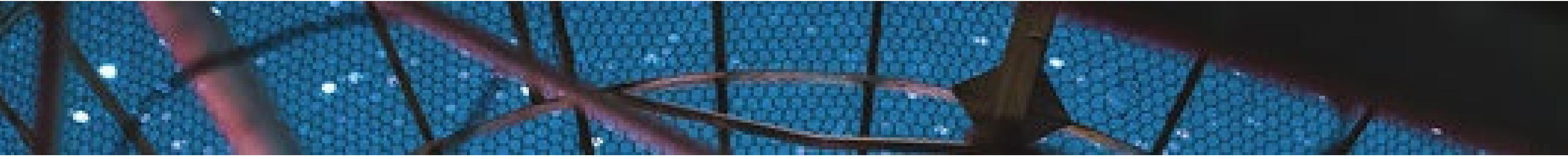
Challenge

CUI and other sensitive data[133] move through cloud platforms, SaaS tools, engineering environments, and subcontractor systems, yet lifecycle governance remains uneven and incomplete. Programs often provide marking guidance without clear instructions for storage, access, retention, sharing, or destruction, particularly in identity-mediated and multi-tenant environments. In the FAST Study questionnaire for the Big 7 (i.e., long-standing DIB primes), 67% reported inconsistent CUI guidance across MILDEPs/CSAs and 63% reported either no clear guidance or unclear documents, forcing DIB primes and subcontractors to infer lifecycle rules and increasing rework of the risk.

Recommended Government Action

The Department should define an authoritative CUI and sensitive data lifecycle model that governs data from origination through final disposition, with OUSW(I&S) responsible for establishing lifecycle governance and policy direction, in coordination with OUSW(A&S) to require explicit

[132] NIST (2011). *NIST SP 800-137: Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*. Source: https://csrc.nist.gov/publications/detail/sp/800-137/final
[133] DOD (2020). *DOD Instruction 5200.48: Controlled Unclassified Information (CUI)*. Source: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/520048p.pdf



lifecycle instructions in acquisition artifacts, including DD-254s[134] and flowdowns, and with the DOW CIO to align technical enforcement to identity-aware access controls consistent with Zero Trust principles.[135] The model should require explicit lifecycle instructions from origination through disposition and provide standardized templates to ensure consistent application across programs. MILDEPs and DCSA should execute this model by implementing consistent templates and applying uniform review expectations across programs.

Impact for Warfighter

Clear lifecycle governance ensures sensitive data remains accessible, protected, and trustworthy across mission systems, reducing operational friction and strengthening data-driven decision-making.

Company Experience: A maritime company described conflict between CUI handling requirements and shipboard operational realities. Vessels relied on shared accounts to support safety and continuity, while CUI guidance assumed individual user identities and enterprise-style access controls. To comply, the company implemented a separate email system exclusively for CUI, increasing complexity, cost, and operational friction. The company emphasized that the requirement was applied without accounting for operational context, introducing new risks while attempting to mitigate others.

56) Fragmented Continuous Monitoring Expectations Prevent Comparable Cyber Risk Decisions

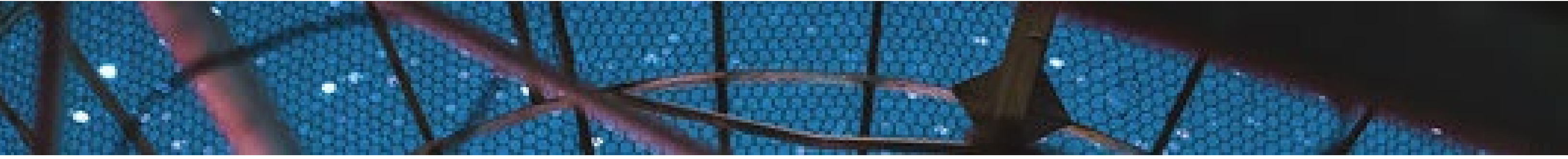
Challenge

Continuous monitoring[136] expectations vary widely across reviewers, with inconsistent requirements for telemetry sources, reporting formats, and update frequency. Cloud-native and provider-managed monitoring is often undervalued or rejected in favor of manual reporting, shifting monitoring away from real-time risk awareness and toward compliance artifact production. In the FAST Study questionnaire, 31% of DIB respondents specifically flagged continuous monitoring as an area where clearer guidance is needed, consistent with the reported variance in reviewer expectations. Cloud service providers and MSPs operate security monitoring capabilities at a scale, depth, and frequency that individual contractors cannot practically replicate, including native visibility into platform-level events, identity activity, configuration state, and service telemetry unavailable to tenant-managed tools.

[134] DCSA (2021). *Contract Security Classification Specification (DD Form 254)*. Source: https://www.dsca.mil/Portals/91/Documents/CTP/DD254.pdf

[135] DOD CIO (2022). *DOD Zero Trust Strategy*. Source: https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf

[136] NIST (2011). NIST SP 800-137: *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*. Source: https://csrc.nist.gov/publications/detail/sp/800-137/final



Recommended Government Action

The Department should implement an architecture-aware continuous monitoring standard that defines acceptable telemetry sources, reporting mechanisms, and escalation paths across cloud, MSP, OT, and legacy environments, with the DOW CIO responsible for defining the authoritative standard, telemetry sufficiency criteria, and accepted reporting mechanisms.

This standard should explicitly recognize that cloud-native and provider-managed telemetry, produced under DOW CIO recognized authorization and continuous monitoring processes, reflects authoritative system behavior at a scale and fidelity not achievable through contractor-generated artifacts alone. Where provider telemetry[137] meets defined sufficiency criteria, it should be treated as authoritative unless mission-specific risk justifies additional validation. Component Authorizing Officials and DCSA reviewers should execute this standard by aligning review checklists and oversight practices to these criteria and by consistently accepting validated provider telemetry as a primary risk signal supporting detection, response, and recovery.

Impact for Warfighter

Consistent monitoring expectations improve visibility into cybersecurity risk while enabling faster response to degradation or attack, strengthening mission resilience.

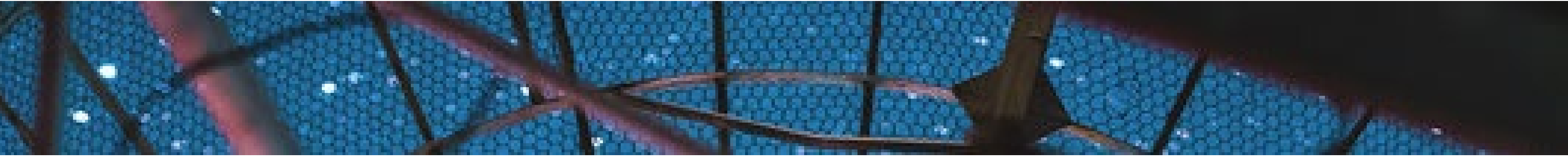
57) Undefined OT Cyber Requirements Disrupt Operations without Improving Security Outcomes

> *"A machine runs 24 hours a day, 7 days a week… downtime is at a cost."* – Council and consortium interviewee

Challenge

OT systems are routinely evaluated using cybersecurity assumptions developed for enterprise IT environments, where systems can be patched frequently, restarted on demand, and temporarily taken offline with limited operational consequence. These assumptions do not hold in OT environments, where systems directly control physical processes, safety-critical equipment, and production lines that must operate continuously and predictably. OT systems often run specialized hardware and software under strict vendor constraints. Many cannot be patched on typical IT timelines without voiding warranties, disrupting calibration, or introducing safety and reliability risks. Active scanning, aggressive configuration changes, or forced reboots that are routine in IT environments can cause equipment faults, production outages, or unsafe operating conditions in OT contexts. As a result, applying IT-style remediation expectations to OT environments frequently creates findings that cannot be resolved without unacceptable operational or safety tradeoffs.

[137] DOD CIO (2023). *DOD Cloud Computing Security Requirements Guide (SRG).* Source: https://dodcio.defense.gov/Portals/0/Documents/Cloud/DOD-Cloud-Computing-SRG-v1r4.pdf



Since existing evaluation criteria do not sufficiently account for these constraints, OT cybersecurity assessments vary widely by reviewer. Identical environments may receive conflicting findings depending on how individual reviewers interpret patching timelines, scanning requirements, or acceptable compensating controls. This inconsistency drives waiver cycles, delays remediation of real risks, and shifts focus away from security measures that are actually effective in OT settings, without materially improving cyber resilience.

Recommended Government Action

The Department should define and implement a distinct OT cybersecurity evaluation framework that recognizes stability and availability as core security properties, with the DOW CIO responsible for defining the authoritative OT evaluation framework and standardized evidence expectations, in coordination with OUSW(A&S) where OT cybersecurity requirements must be integrated into acquisition planning and sustainment realities.

This framework should explicitly account for vendor-imposed constraints, safety considerations, and continuous operational requirements that limit the applicability of frequent patching, active scanning, and downtime-based remediation common in IT environments. It should emphasize isolation, segmentation, passive monitoring, and compensating controls as risk-equivalent security measures rather than prescriptive IT remediation. Evidence expectations and reviewer criteria should be standardized to ensure consistent, risk-based evaluation of OT environments, ensuring that alternative controls provide security outcomes commensurate with IT requirements. Component Authorizing Officials and DCSA reviewers should execute this framework by applying OT-appropriate criteria, such as segmentation, passive monitoring, and compensating controls, rather than defaulting to IT-centric remediation approaches.

Impact for Warfighter

Aligned OT cybersecurity oversight protects critical production, testing, and sustainment operations without introducing unnecessary downtime or safety risk. By focusing on controls that reflect how OT systems actually operate, the Department improves the resilience and reliability of mission-essential capabilities while reducing delays and disruption to warfighter support.

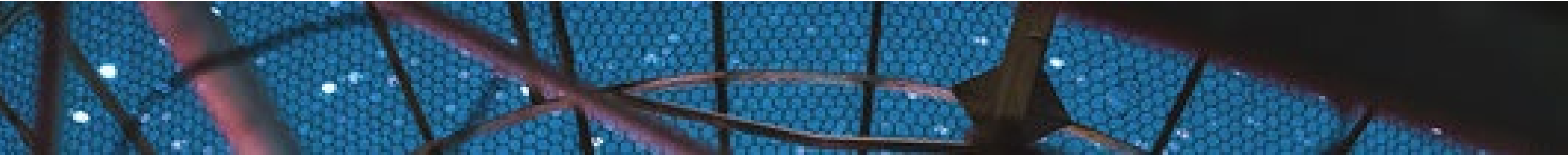
58) Misaligned Logging and Audit Expectations Exceed Capabilities of Cloud, MSP, OT, and Legacy Systems

> *"We don't have the logs they're asking for. The system was never built to record that kind of detail."* – Industry interviewee

Challenge

Logging and audit expectations remain inconsistent and frequently disconnected from modern detection and response practices.[138] Reviewers often expect uniform log outputs across systems

[138] NIST (2022). *NIST SP 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations.* Source: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final



with vastly different technical capabilities, including cloud, MSP, OT, and legacy platforms, resulting in compliance-driven logging that does not meaningfully support security operations.

In addition, DOW does not currently have User Activity Monitoring (UAM) capabilities on unclassified systems (e.g., NIPRNet). Despite the Joint Management Office for Insider Threat and Cyber Capabilities being established in 2023,[139]the UAM capability has still not been purchased and deployed in any widespread manner. The lack of UAM on DOW unclassified systems creates significant risk for both the proactive detection of insider risks and threats such as unauthorized disclosures, and forensic analysis of insider threats. UAM solutions and practices are increasingly implemented on industry IT systems, meaning DOW is behind the industry baseline. Classified UAM programs are policy-mandated (e.g., EO 13587, NISPOM 1-202 and 1-300), but actual deployment of technical capabilities such as UAM or UEBA lags for unclassified networks where there are arguably better potential risk indicators to monitor and detect.

Recommended Government Action

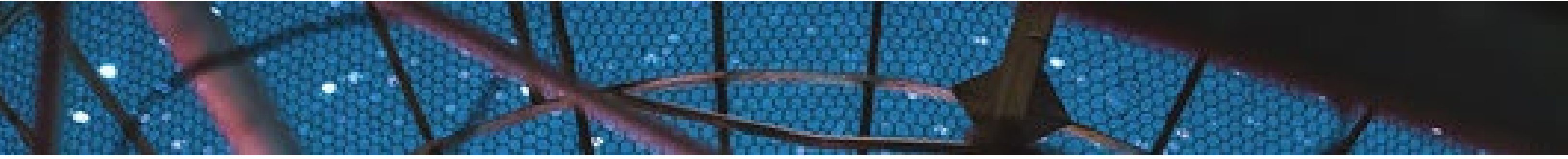
The Department should implement standardized, outcome-oriented telemetry and logging requirements aligned to threat detection, incident response, and mission impact. Provider-managed and platform telemetry should be treated as authoritative[140] with the DOW CIO responsible for defining outcome-oriented telemetry and logging sufficiency standards aligned to detection, response, and mission impact, in coordination with OUSW(I&S) where oversight expectations are set through industrial security policy interpretations. Provider-managed and platform telemetry should be treated as authoritative where validated, and sufficiency should be evaluated based on security outcomes rather than log volume or format. Component Authorizing Officials and DCSA reviewers should execute this approach by evaluating logging against outcome-oriented criteria and accepting validated platform and provider telemetry as authoritative where appropriate. The DOW should also rapidly deploy UAM on unclassified systems to proactively identify unauthorized disclosure and other insider risks or threats within each of the MILDEPs.

Impact for Warfighter

Improved telemetry standards enhance detection and response speed while reducing delays caused by low-value logging demands, strengthening operational resilience.

[139] Secretary of Defense (2023). *Security Review Follow-on Actions.* Source: https://media.defense.gov/2023/Jul/05/2003253531/-1/-1/1/SECURITY-REVIEW-FOLLOW-ON-ACTIONS.PDF

[140] DOD CIO (2023). *DOD Cloud Computing Security Requirements Guide (SRG)*. Source: https://dodcio.defense.gov/Portals/0/Documents/Cloud/DOD-Cloud-Computing-SRG-v1r4.pdf



59) Configuration Management Requirements Conflict with Provider-Managed and OT Environments

> *"We can't change the configuration… the vendor locks it down and any modification breaks certification."* – Council and consortium interviewee

Challenge

Configuration management expectations[141] remain anchored to assumptions from traditional, contractor-owned IT environments where all layers of the stack could be uniformly controlled. Today's systems span cloud platforms, MSP-managed infrastructure, OT environments, and legacy equipment, each with fundamentally different configuration authority and technical constraints. Contractors frequently lack the ability to modify provider-managed baselines, alter vendor-certified OT firmware, or instrument legacy systems without jeopardizing operations. As a result, assessments often conflate technical infeasibility with noncompliance, and configuration evidence that is accepted in one context is rejected in another.

Recommended Government Action

The Department should develop an environment-aware configuration management framework that defines how configuration responsibilities and expectations map across cloud, MSP, OT, and legacy systems, with the DOW CIO responsible for defining the authoritative framework, the evidence model for inherited and provider-managed baselines, and criteria for evaluating compensating controls, in coordination with OUSW(A&S) where vendor lock-in and certification constraints must be reflected in acquisition strategy. The framework should clarify which configuration elements are contractor-controlled versus provider-controlled and define acceptable evidence for inherited baselines, including provider attestations, hardened images, and continuous configuration drift monitoring.[142]

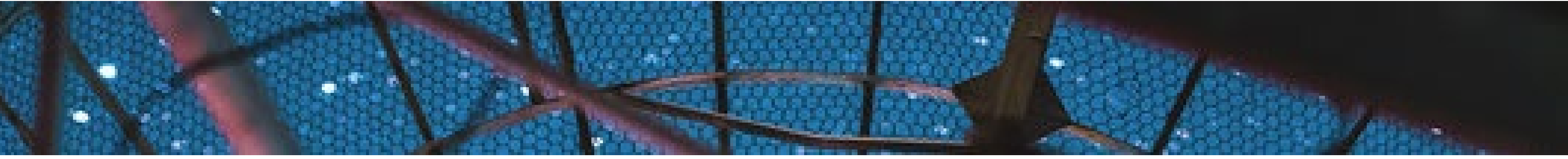
Reviewer training should be unified across MILDEPs and DCSA regions to ensure consistent interpretation. Component Authorizing Officials and DCSA reviewers should execute this framework by standardizing reviewer interpretation and avoiding treatment of infeasibility as noncompliance when compensating controls are appropriate.

Impact for Warfighter

When configuration management expectations do not align with technical reality, programs misaligned configuration expectations drive avoidable delays as programs spend time reconstructing evidence rather than improving security posture. A configuration management framework grounded in architectural reality accelerates authorization timelines, supports stable

[141] NIST (2022). *NIST SP 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations*. Source: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

[142] NIST (2011). *NIST SP 800-137: Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*. Source: https://csrc.nist.gov/publications/detail/sp/800-137/final



and maintainable systems, and ensures mission capabilities reach the field without being stalled by unrealistic compliance demands.

60) RMF Processes Fail to Align with Modern, Distributed Architectures

Challenge

Program protection decisions such as CPI, CTI, CUI, and classification determinations, are frequently made late and are not systematically translated into cybersecurity architectures or RMF baselines. Even when protection artifacts exist, cybersecurity design, cloud and MSP patterns, boundary definitions, and control baselines often proceed independently, based on generic assumptions rather than the program's declared protection priorities. As a result, RMF artifacts, system architectures, and monitoring strategies do not consistently reflect what the Department has identified as most critical to protect.

Recommended Government Action

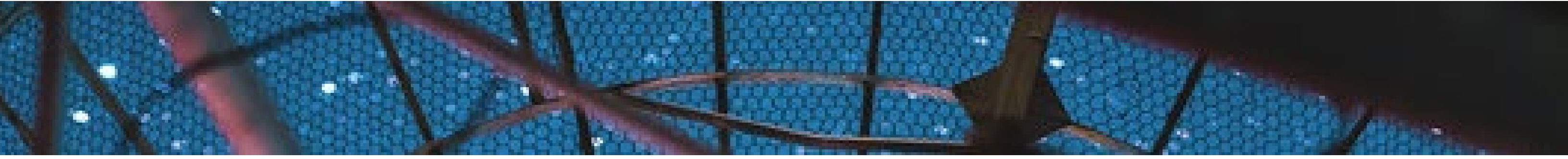
The Department should implement a mandatory, repeatable mechanism requiring cybersecurity architectures and RMF baselines to be explicitly derived from the Program Protection Baseline,[143] with governance responsibilities jointly aligned across the DOW CIO, OUSW(I&S), and OUSW(A&S). Under this approach, the DOW CIO should define requirements linking RMF and cyber architecture decisions to program protection baselines, OUSW(I&S) should provide authoritative protection policy inputs, classification guidance,[144] and OUSW(A&S) should ensure integration and enforcement through acquisition planning and program baselines. Programs should be required to demonstrate how CPI, CTI, CUI, and classification decisions map into system boundaries, enclave and segmentation choices, use of cloud and MSP services, inherited controls, and monitoring expectations. When protection artifacts are updated, programs should revisit and adjust cyber architectures and RMF documentation accordingly. Component Authorizing Officials and DCSA reviewers should execute this mechanism by enforcing consistent linkage between PPBs RMF decisions, system boundaries, and continuous monitoring expectations.

Impact for Warfighter

When cybersecurity is not derived from the protection baseline, systems reach the field with misaligned security posture and unclear risk priorities, leading to authorization delays and late redesign. Enforcing a clear linkage between protection decisions and cyber implementation accelerates delivery, improves oversight predictability, and ensures mission systems are secured in accordance with what the Department has determined truly matters.

[143] DOD (2020). *DOD Instruction 5200.44: Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)*. Source: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/520044p.pdf

[144] DOD (2020). *DOD Instruction 5200.48: Controlled Unclassified Information (CUI)*. Source: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/520048p.pdf



61) Fragmented System Boundary Definitions Produce Conflicting Cyber Requirements for Identical Architectures

> *"Every program draws the boundary differently, and somehow we're the ones who have to guess which version they meant."* – Industry interviewee

Challenge

System boundary definitions vary widely across reviewers and often shift during authorization, even for unchanged architectures.[145] Legacy perimeter-based assumptions are frequently applied to cloud, MSP, hybrid, and OT environments, creating uncertainty that directly affects logging scope, inheritance decisions, scanning expectations, and identity enforcement.[146]

Recommended Government Action

The Department should define and enforce a unified boundary determination framework aligned to modern architectures and Zero Trust principles.[147] The DOW CIO, in coordination with OUSW(A&S) to require boundary determination early in acquisition planning and artifacts, should define an authoritative boundary framework aligned to ZT and modern architecture patterns and require boundaries to be established early in acquisition planning, explicitly document shared-responsibility layers, and be locked unless material architectural changes occur. Component Authorizing Officials and DCSA reviewers should execute this framework by evaluating boundary determinations consistently across MILDEPs and carrying forward those determinations absent material architectural change." To ensure consistent application, the Department should develop and require Department-wide training on the unified boundary determination framework so that MILDEP reviewers, Authorizing Officials, and DCSA personnel evaluate boundaries strictly in accordance with the authoritative framework rather than MILDEP-specific interpretations.

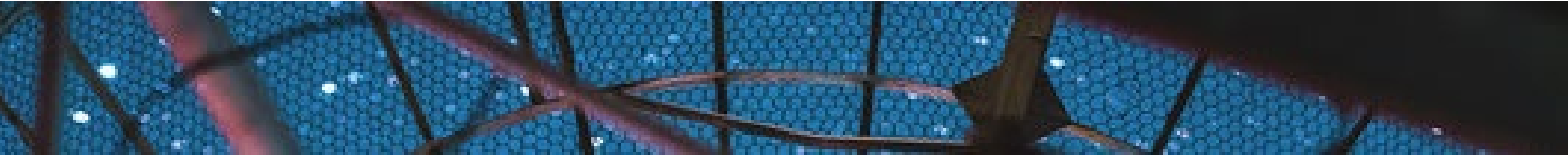
Impact for Warfighter

Stable, architecture-aware boundaries reduce rework and enable predictable fielding of mission systems without sacrificing cyber rigor or operational security.

[145] DOD (2022). *DOD Instruction 8510.01: Risk Management Framework (RMF) for DOD Systems*. Source: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/851001p.pdf

[146] DOD CIO (2020). *DOD Identity, Credential, and Access Management (ICAM) Strategy*. Source: https://dodcio.defense.gov/Portals/0/Documents/Cyber/ICAM_Strategy.pdf

[147] DOD CIO (2022). *DOD Zero Trust Strategy*. Source: https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf



62) Disjointed Threat Intelligence Sharing Limits Collective Defense Across the DIB

> *"We get threat briefs, but nothing we can actually use. They tell us what happened, not what to do about it."* – Industry interviewee
>
> *"Government shares indicators after the fact. We need them when they matter."* – Industry interviewee
>
> *"Everyone says 'share more,' but no one will say what's allowed or who owns the risk of sharing."* – Council and consortium interviewee
>
> *"We're all trying to defend the same ecosystem, but everyone's looking through a different keyhole."* – Industry interviewee

Challenge

Cyber threat intelligence provided to the DIB is frequently too late, too vague, too classified, or too disconnected from defensive action to be operationally useful.[148] Practices vary widely by program, and contractors, especially mid-tier companies, MSPs, and subcontractors, that often lack timely, actionable indicators they can apply.[149] Unclear or contradictory rules about what may be redistributed (and under whose authority[150]) further prevent DIB primes from sharing indicators with subcontractors and service providers, resulting in a fragmented and reactive defensive posture across the ecosystem.

Recommended Government Action

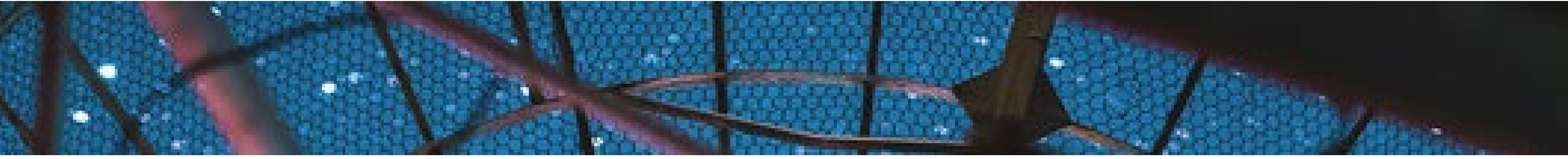
The SecWar should implement an enterprise-wide, repeatable model for delivering actionable cyber threat intelligence across the DIB with the speed required to outpace active campaigns, using unclassified tear lines whenever possible, with OUSW(I&S) responsible for defining threat intelligence policy, tear-line posture, and sharing authorities, in coordination with DOW CIO to ensure delivery formats are compatible with modern security tools and integrated with continuous monitoring workflows, and with OUSW(A&S) to align contractual expectations and flowdowns to primes, subcontractors, and MSPs. Indicators should be provided in formats compatible with modern security tools (e.g., STIX/TAXII) rather than through episodic briefings or static reports.

Ownership and sharing authority should be clearly defined so contractors understand what may be shared, with whom, in what form, and under what contractual basis. Threat intelligence expectations should be woven into the broader governance structure, including DD-254s, program protection elements, continuous monitoring activities, and subcontractor flowdowns, to ensure

[148] DHS OIG (2025). *CISA Has Not Finalized Plans for Automated Cyber Threat Indicator Sharing.* Source: https://www.oig.dhs.gov/sites/default/files/assets/2025-09/OIG-25-46-Sep25.pdf

[149] CISA (n.d.). *Automated Indicator Sharing (AIS) Service.* Source: https://www.cisa.gov/resources-tools/services/automated-indicator-sharing-ais-service

[150] Congressional Research Service (2025). *The Cybersecurity Information Sharing Act of 2015.* Source: https://www.congress.gov/crs-product/IF12959



consistent implementation across programs.[151] MILDEPs and DCSA should execute this model by enforcing consistent implementation through DD-254s, program protection artifacts, and subcontractor mechanisms.

Impact for Warfighter

When threat intelligence is delayed, inconsistent, or unusable, adversaries exploit seams in the supply chain before coordinated defenses can mobilize, increasing the risk of compromise that affects mission capability. A unified, timely model enables coordinated defensive action across DIB primes, subcontractors, and service providers, strengthening the resilience of the industrial base that warfighters rely on.

63) Facility-Centric Cyber Models Fail to Support Emerging Mission Geographies

Challenge

Defense missions increasingly operate across distributed, hybrid environments such as spaceports, and other commercial launch facilities, test ranges, and blended civil–military campuses that rely on cloud platforms, digital telemetry, remote operations centers, and geographically dispersed teams. Yet oversight frameworks remain anchored to facility-centric[152] assumptions involving static boundaries, fixed accreditations, and linear review processes. As a result, cyber and security expectations do not align with the geography, tempo, or architecture of modern mission operations, creating uncertainty, rework, and delay.[153]

Recommended Government Action

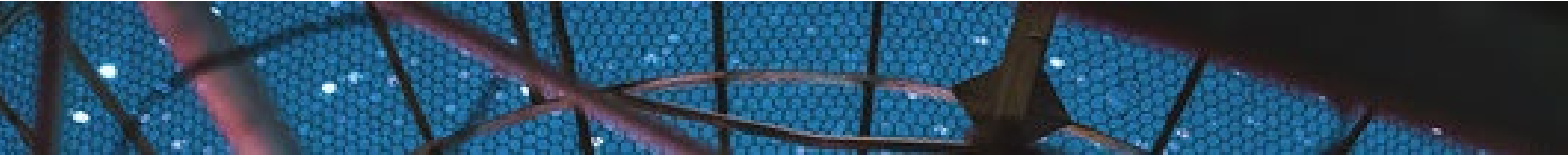
The Department should implement a governance model that treats emerging mission geographies as operational constructs rather than exceptions to legacy facility frameworks, with joint responsibility across OUSW(A&S), DOW CIO, and OUSW(I&S). Under this model, OUSW(A&S) should operationalize oversight expectations through acquisition constructs and mission partnerships, DOW CIO should define cybersecurity expectations for distributed and digital mission environments, and OUSW(I&S) should ensure classification management and industrial security governance are appropriately aligned for non-traditional mission sites, including hybrid commercial–government operations,[154] so that these environments are evaluated consistently rather than as exceptions. Standardized guidance and reviewer playbooks should be provided so that evaluation of non-traditional mission sites becomes predictable, consistent, and aligned to operational reality. MILDEPs and DCSA should execute this model by applying standardized playbooks and consistent review criteria across non-traditional mission sites.

[151] DOD (2025). *Title 32—National Defense, Part 236: Defense Industrial Base (DIB) Cybersecurity (CS) Activities.* Source: https://www.govinfo.gov/link/cfr/32/236?link-type=pdf&year=mostrecent

[152] DOD (2020). *National Industrial Security Program Operating Manual (NISPOM)*. 32 CFR Part 117. Source: https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-D/part-117

[153] The White House (2025). *National Security Strategy of the United States of America*. Source: https://www.whitehouse.gov/wp-content/uploads/2025/12/2025-National-Security-Strategy.pdf

[154] CISA (2023). *Defense Industrial Base Sector-Specific Plan*. Source: https://www.cisa.gov/dib-sector



Impact for Warfighter

When oversight models fail to reflect modern mission geographies, operational units experience delays, missed launch windows, and friction that undermines mission tempo. Aligning governance to distributed mission environments accelerates integration, improves predictability for mission partners, and enables warfighters to receive capabilities on timelines dictated by operational need rather than outdated constructs.

Modern Cybersecurity Framework for the NISP Era

The cybersecurity challenges consistently observed by industry show a system built for a world that no longer exists and one that is impeding their ability to deliver the capabilities necessary for modern warfare and defense. The legacy NISP model presumes stable boundaries, contractor-owned infrastructure, locally administered systems, and slow technology cycles. Today's defense missions run on cloud and SaaS platforms, MSP-managed environments, federated identity, OT/ICS systems tied to physical consequences, and distributed mission complexes that cross government, commercial, and contractor infrastructure.

DOW leadership described this shift with clarity:

- ZT is not optional.
- Visibility and telemetry are foundational.
- Fragmented governance, legacy architectures, and inconsistent baselines are now strategic risks.
- Standardization is no longer optional.

The FAST Study's evidence demonstrates these conditions at scale. Cybersecurity cannot be overseen through screenshots, isolated interpretations of cloud or inheritance, or facility-centric models that misalign with modern architectures. The NISP requires a cybersecurity framework that reflects how systems are actually built, secured, and operated in 2025; and one that supports predictable, repeatable outcomes across the entire DIB. Modernization efforts must avoid locking in architectures that satisfy current controls but fail to meet near-term federal security expectations. Interviewees warned that this misalignment already shapes design decisions. As one C3PAO put it, "*We are conforming to an interpretation of 800-171 that will not survive the next five years. We are building to pass the test, not to survive the threat.*" A viable NISP cybersecurity framework must support forward compliance so that systems implemented today remain defensible as assurance standards evolve.

The modernization pathway must translate the FAST Study cybersecurity recommendations into a coherent architectural foundation that:

1. Defines cybersecurity in architectural terms, not checklist terms.
2. Replaces static documentation with authenticated telemetry and real evidence.
3. Standardizes models for cloud, SaaS, identity, MSPs, OT/ICS, and data lifecycle.
4. Integrates cybersecurity expectations early in acquisition, not after design decisions are locked.
5. Measures success in mission continuity and survivability, not procedural compliance.

These principles form the basis of the modernization pillars that follow. The pillars are not abstractions; they are the structural requirements needed for the NISP to operate in the current environment and for the Department to ensure secure, resilient participation from its industrial base. They represent the conditions under which modern missions can be protected, and the only conditions under which the NISP can remain viable in the decade ahead.

Moving DOW toward an Integrated Cybersecurity Enterprise Model

For more than a decade, the Department has accumulated cybersecurity policies layer upon layer, each well-intentioned, each created to address a discrete need, and none designed to harmonize with what came before or after. The result is an oversight ecosystem that behaves less like a coordinated system of controls and more like a constellation of overlapping mandates, interpretations, and exceptions that vary with every program office, every reviewing authority, every accrediting body, and often every individual assessor. Within the NISP, this fragmentation becomes especially consequential. Contractors already operate inside a heavily conditioned environment, and any misalignment in cybersecurity expectations multiplies across their cloud providers, MSP relationships, subcontractors, and mission partners. Cybersecurity, in this world, is not simply another requirement, they experience it as the terrain itself.

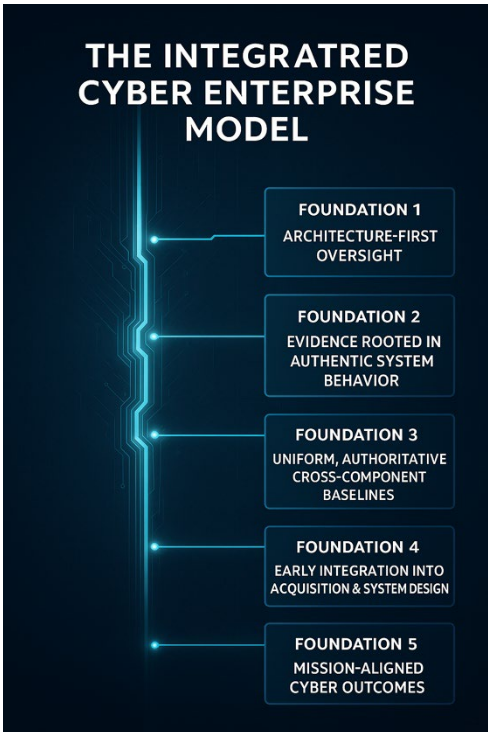

THE INTEGRATRED CYBER ENTERPRISE MODEL
FOUNDATION 1
ARCHITECTURE-FIRST OVERSIGHT
FOUNDATION 2
EVIDENCE ROOTED IN AUTHENTIC SYSTEM BEHAVIOR
FOUNDATION 3
UNIFORM, AUTHORITATIVE CROSS-COMPONENT BASELINES
FOUNDATION 4
EARLY INTEGRATION INTO ACQUISITION & SYSTEM DESIGN
FOUNDATION 5
MISSION-ALIGNED CYBER OUTCOMES

Figure 7. Integrated Cyber Enterprise Model

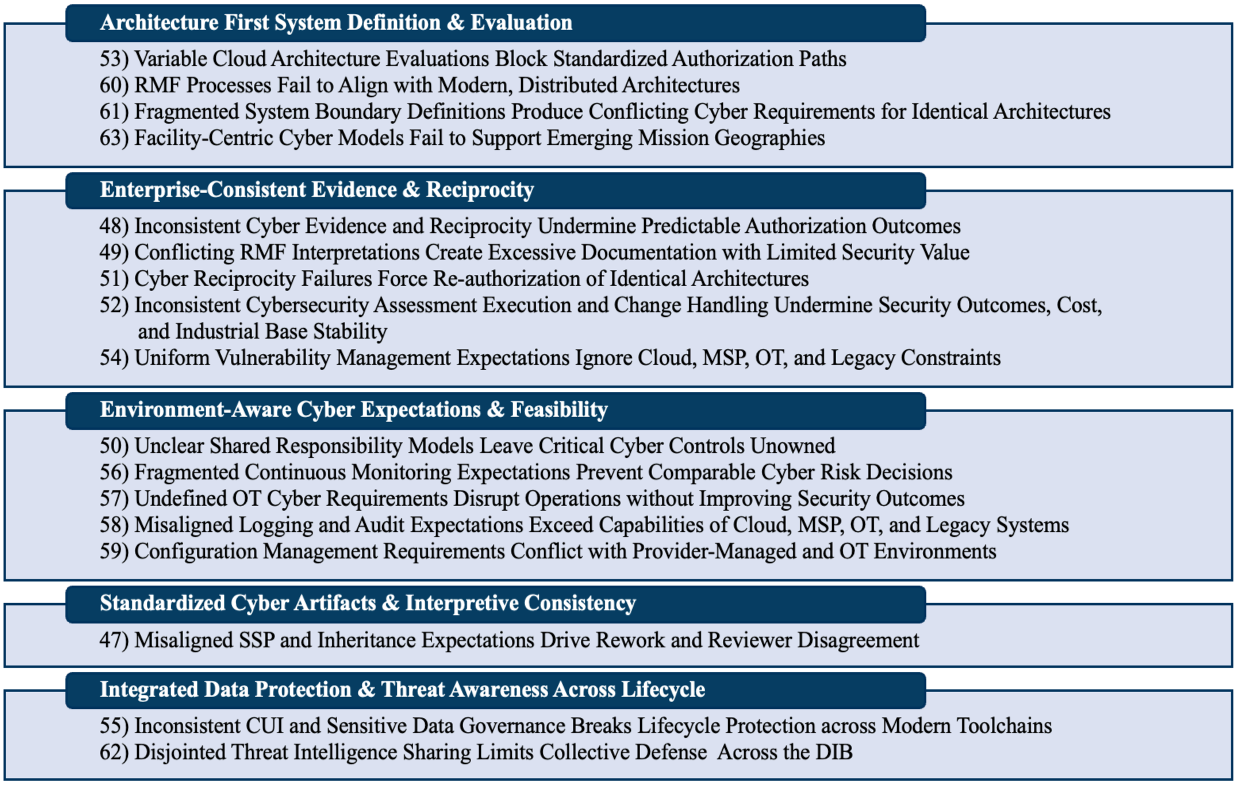
This section identifies five foundational elements that must anchor a modernized NISP Integrated Cybersecurity Enterprise Model, depicted above in Figure 7. These elements are not conceptual ideals; they are the structural requirements implied directly by the evidence gathered across the FAST Study cybersecurity challenges and recommended actions:

1. **Architecture-First Oversight:** FAST Study interviews revealed identical systems are repeatedly audited afresh because oversight is focused on artifacts rather than on shared architectural patterns. Modern environments, cloud, MSP-administered stacks, SaaS platforms, OT/ICS systems, operate as integrated ecosystems. A modern model must evaluate architectures, not artifacts.
2. **Evidence Rooted in Authentic System Behavior:** Monitoring practices across MILDEPs remain built on screenshots and static documentation, models fundamentally incapable of validating configuration, identity behavior, or privilege governance. Modern oversight must rely on telemetry and authenticated system behavior.
3. **Uniform, Authoritative Cross-MILDEP Baselines:** FAST Study found that cloud approvals, ZT expectations, MSP responsibilities, OT constraints, and data-lifecycle rules vary dramatically across MILDEPs and regions, driving delay and rework. A modern model requires clear, consistent, cross-MILDEP baselines.

4. **Early Integration into Acquisition and System Design:** Cyber requirements often arrive after architectures and contracts are fixed, creating structural misalignment that no amount of documentation can resolve. Modern oversight must begin where architectures begin.
5. **Mission-Aligned Cybersecurity Outcomes:** Cybersecurity risk must be assessed in terms of mission behavior, not paperwork compliance. Mission owners emphasized that continuity, resilience, and threat-informed understanding are essential for operational viability.

These five foundational elements, depicted in Figure 8 translate the 17 isolated challenges into a coherent architectural model for a modernized NISP. They define the structural conditions under which oversight becomes predictable, evidence becomes meaningful, small businesses can participate reliably, and missions can withstand the realities of modern threats.

The 2025 National Security Strategy[155] warns that adversaries are working relentlessly to undermine these foundations, and the cybersecurity strategy reinforces that the United States must "shape adversary behavior by imposing costs and consequences." That only becomes possible when the DOW enterprise operates from a common architecture instead of a patchwork of local interpretations.



Architecture First System Definition & Evaluation

53) Variable Cloud Architecture Evaluations Block Standardized Authorization Paths
60) RMF Processes Fail to Align with Modern, Distributed Architectures
61) Fragmented System Boundary Definitions Produce Conflicting Cyber Requirements for Identical Architectures
63) Facility-Centric Cyber Models Fail to Support Emerging Mission Geographies

Enterprise-Consistent Evidence & Reciprocity

48) Inconsistent Cyber Evidence and Reciprocity Undermine Predictable Authorization Outcomes
49) Conflicting RMF Interpretations Create Excessive Documentation with Limited Security Value
51) Cyber Reciprocity Failures Force Re-authorization of Identical Architectures
52) Inconsistent Cybersecurity Assessment Execution and Change Handling Undermine Security Outcomes, Cost, and Industrial Base Stability
54) Uniform Vulnerability Management Expectations Ignore Cloud, MSP, OT, and Legacy Constraints

Environment-Aware Cyber Expectations & Feasibility

50) Unclear Shared Responsibility Models Leave Critical Cyber Controls Unowned
56) Fragmented Continuous Monitoring Expectations Prevent Comparable Cyber Risk Decisions
57) Undefined OT Cyber Requirements Disrupt Operations without Improving Security Outcomes
58) Misaligned Logging and Audit Expectations Exceed Capabilities of Cloud, MSP, OT, and Legacy Systems
59) Configuration Management Requirements Conflict with Provider-Managed and OT Environments

Standardized Cyber Artifacts & Interpretive Consistency

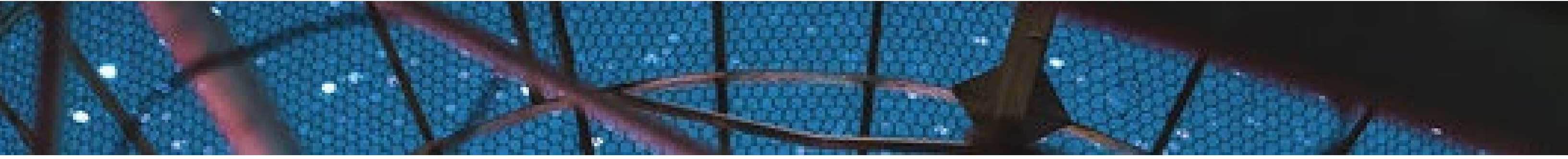
47) Misaligned SSP and Inheritance Expectations Drive Rework and Reviewer Disagreement

Integrated Data Protection & Threat Awareness Across Lifecycle

55) Inconsistent CUI and Sensitive Data Governance Breaks Lifecycle Protection across Modern Toolchains
62) Disjointed Threat Intelligence Sharing Limits Collective Defense Across the DIB

Figure 8. Foundational Elements of a Modernized NISP Cybersecurity Framework

[155] The White House (2025). *National Security Strategy of the United States of America*. Source: https://www.whitehouse.gov/wp-content/uploads/2025/12/2025-National-Security-Strategy.pdf



Looking Ahead

The Department now faces a choice: continue treating cybersecurity as a cross-cutting but ungoverned set of obligations, or acknowledge that cybersecurity requires its own coherent center of gravity, a place where interpretations are harmonized, inheritance is defined, evidence models are standardized, and mission-relevant expectations evolve in sync with the technology environment they regulate.

The FAST Study data highlight the consequences when no such authority exists. Contractors described near-identical systems evaluated entirely differently by different MILDEPs. MSPs noted that they lacked a clear standard for what “inheritance” means in NISP, CMMC, or RMF contexts. Cloud providers described federal customers who treat FedRAMP as both authoritative and insufficient depending on the day and the reviewer. Government personnel themselves admitted they often inherit unresolved contradictions, forcing them to rely on judgment rather than clear guidance. No one is acting improperly. They are navigating a system that does not provide shared footing.

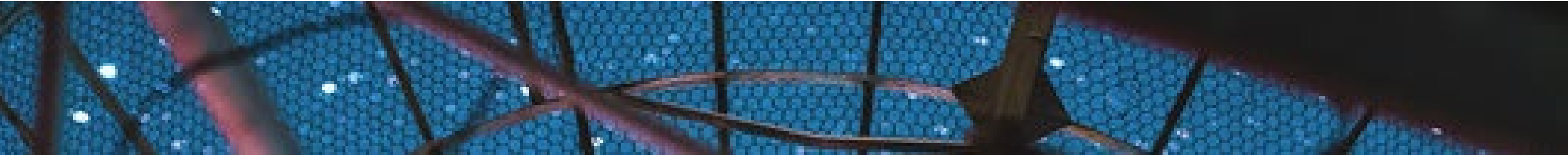
The Integrated Cybersecurity Enterprise Model changes this dynamic by establishing a consistent interpretive foundation while preserving the specific value each domain brings. It must define what is mandatory, what is inherited, what is reviewed once, and what is reviewed always. And it must ensure that policy evolution, in Zero Trust, cloud, MSP oversight, OT security, identity federation, telemetry, incident reporting, is synchronized across the enterprise, not reshaped independently by each MILDEP or review team. Such governance is not a new layer; it is the removal of dozens of unnecessary layers that currently obscure the Department’s intent and overwhelm the industrial base.

The cybersecurity reforms articulated through the 17 FAST Study cybersecurity challenges with recommended government actions represent a transformation in how the Department conceives of, executes, and measures cybersecurity across the industrial base. It enables the NISP to evolve from a facility-centric construct built for a Cold War threat environment into a dynamic enterprise-security model capable of handling the distributed, cloud-enabled, highly interconnected defense ecosystem that defines modern missions. Companies gain a predictable pathway to participate. Government gains a defensible, data-driven oversight model. Mission owners gain assurance that cybersecurity posture reflects mission survivability, not documentation completeness.

The FAST Study’s recommended government actions are about making the system coherent, predictable, aligned, and mission-ready. Cybersecurity is no longer a subsection of industrial security. It is industrial security, and the FAST Study now gives DOW a pathway to modernize it. DOW does not get to choose between secure systems and fast systems. The adversary forces the DIB to build systems that are both.

CYBERSECURITY INDUSTRY CHALLENGES

1. Misaligned System Security Plans and Inheritance Expectations Drive Rework and Reviewer Disagreement
2. Inconsistent Cyber Evidence and Reciprocity Undermine Predictable Authorization Outcomes
3. Conflicting RMF Interpretations Create Excessive Documentation with Limited Security Value
4. Unclear Shared Responsibility Models Leave Critical Cyber Controls Unowned
5. Cyber Reciprocity Failures Force Re-authorization of Identical Architectures
6. Inconsistent Cybersecurity Assessment Execution and Change Handling Undermine Security Outcomes, Cost, and Industrial Base Stability
7. Variable Cloud Architecture Evaluations Block Standardized Authorization Paths
8. Uniform Vulnerability Management Expectations Ignore Cloud, MSP, OT, and Legacy Constraints
9. Inconsistent CUI and Sensitive Data Governance Breaks Lifecycle Protection across Modern Toolchains
10. Fragmented Continuous Monitoring Expectations Prevent Comparable Cyber Risk Decisions
11. Undefined OT Cyber Requirements Disrupt Operations without Improving Security Outcomes
12. Misaligned Logging and Audit Expectations Exceed Capabilities of Cloud, MSP, OT, and Legacy Systems
13. Configuration Management Requirements Conflict with Provider-Managed and OT Environments
14. RMF Processes Fail to Align with Modern, Distributed Architectures
15. Fragmented System Boundary Definitions Produce Conflicting Cyber Requirements for Identical Architectures
16. Disjointed Threat Intelligence Sharing Limits Collective Defense Across the DIB
17. Facility-Centric Cyber Models Fail to Support Emerging Mission Geographies



INTEGRATION OF SECURITY INTO ACQUISITION PROCESSES AND CONTRACTS

Acquisition, security, and program offices are not collaborating to the extent necessary—missing opportunities to effectively integrate security throughout the acquisition lifecycle. Security personnel, program offices, and acquisition/contracting organizations should integrate and collaborate throughout the DOW acquisition process to ensure protection of information, technology, and mission readiness. More effective collaboration can be facilitated by using Cross-Functional Trainings (CFTs) throughout the acquisition lifecycle, leading the different roles to understand the critical benefits of cross-functional teaming. A CFT approach is also part of the Department's broader Acquisition Transformation Strategy[156] (hereafter referred to as DATS) which creates the opportunity for DATS subsequent planning and implementation stages to require CFTs to include acquisition security professionals and security offices, and optionally to include "external" organizations such as DCSA.

> CFT includes elements such as "peer-group learning; simulations and gaming; and expanded participation for CFTs to incorporate representatives from international acquisition, cybersecurity, requirements development, and industry groups." – *DATS*

To ensure effective and enduring CFTs and teaming, they should adhere to best practices to avoid becoming a mere formality (checkbox) or "just another meeting." For instance, CFTs and cross-functional team meetings can include breakout sessions as needed, enabling the team members, including security, to form single or multidiscipline subgroups to address specific topics in parallel. These discussions enable real-time resolutions within subgroups, which can then be shared and discussed timely with the broader cross-functional team during the latter part of the meeting, expediting decisions and document completion. Cross-functional teams could also invite DCSA participation, as needed, to avail the team of DCSA's successful strategies and lessons learned for solutions for similar acquisitions. Additionally, DCSA's participation could help DCSA monitor potential requests, forecast staffing needs, and give DCSA an opportunity to better understand program missions when supporting Entity Clearance and FOCI requirements.

Going forward, it is critical that acquisition strategies and plans obtain security review and concurrence, or approval. This will ensure visibility into the acquisition and avail the program and contracting offices of security expertise at the beginning phases of the acquisition process. This sets a foundation that will facilitate integrating security requirements and considerations throughout the pre- and post-award phases for secure mission assurance.

Security should also be involved during requirements development and when drafting the Work Statement (Statement of Objectives, Performance Work Statement, Statement of Work) and relevant security-related performance measures. Their involvement helps ensure the resulting

[156] DOW (2025). *Acquisition Transformation Strategy: Rebuilding the Arsenal of Freedom*. Source: https://media.defense.gov/2025/Nov/10/2003819441/-1/-1/1/ACQUISITION-TRANSFORMATION-STRATEGY.PDF

services and deliverables meet security guidelines and that the performance measures incentivize secure rapid delivery. Acquisition security professionals can assist with drafting security-related instructions to offerors and evaluation factors/criteria so that offerors are required to propose their approach to security in their technical/security proposal and in their price/cost proposal. Lastly, there should be a review process for security offices (if not already part of a CFT review process) to review RFPs/solicitations and contracts prior to issuance to ensure required/desired security language is complete and accurate. This should also remove ambiguity and reduce questions from offerors.

To complete this integration, acquisition security professionals should be members of the proposal evaluation team in some capacity (e.g., voting member or advisor) based on the acquisition and the evaluation factors or volume structure (if security has its own volume). At a minimum, the evaluation would benefit from acquisition security professionals assessing the security and "technical" alignment within the offeror's proposed solution and alignment with the solicitation guidelines.

Integrating security across solicitation (including pre-solicitation and evaluation) and contract award protects programs from costly vulnerabilities during contract performance. Prioritizing CMMC-aligned cyber resilience, SCRM, and quantifiable post-award metrics, reinforced by DFARS clauses and security-linked incentives, transforms compliance into strategic value. These practices exemplify the 2022 DOW Source Selection Procedures' intent to "deliver quality and timely products and services to the Warfighter and the Nation at the best value for taxpayer."[157] The DOW Ground-Based Strategic Deterrent (GBSD) Program is an example of successfully integrating security into the acquisition process. By embedding the Cyber Resiliency Office for Weapon Systems (CROWS) and Mission Defense Operations Center (MDOC) into acquisition planning, source selection, and system engineering, GBSD improved program resilience and reduced cybersecurity risk exposure in post-award operations.[158]

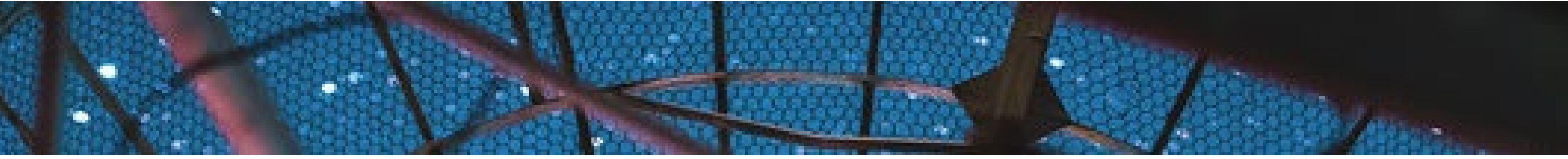
Acquisition Workforce

Security plays multiple roles throughout the DOW acquisition process, requiring continuous integration to ensure protection of information, technology, and mission readiness. It is critical OUSW(A&S) ensures each program or acquisition team has qualified staff (e.g., acquisition security professionals) to achieve security integration throughout the acquisition lifecycle.

> *"The USG (DOW and IC community in particular) have been experiencing a rapid decline in their acquisition work force which is having a direct impact to acquisition timelines. My guess is keeping a workforce with security expertise is also being challenged."*
> – Industry interviewee

[157] DOD (2024). *Source Selection Procedures.* Source: https://www.acq.osd.mil/dpap/policy/policyvault/USA000740-22-DPC.pdf

[158] DOD (2021). *Cybersecurity for DOD Acquisition Program Execution: Best Practices for the Major Capability Acquisition Pathway Insights from the Ground Based Strategic Deterrence (GBSD) Program*. Source: https://www.acq.osd.mil/asda/pwpm/docs/dau/Cybersecurity_Best_Practice_Guidebook_Version_1-24Nov2021.pdf Cybersecurity_Best_Practice_Guidebook_Version_1-24Nov2021.pdf

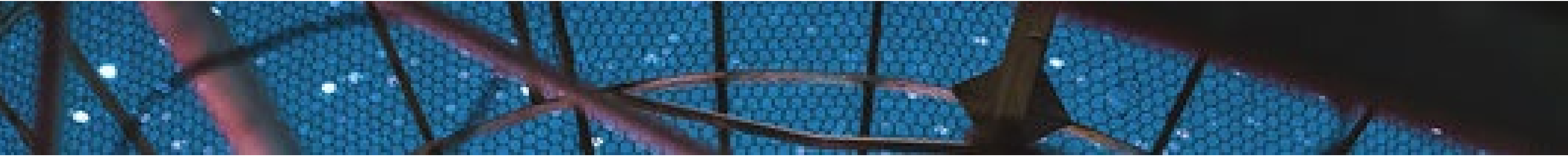


> *"The Under Secretary of War for Acquisition and Sustainment (USW(A&S)) will develop the tools, best practices, and training to ensure PAEs and program management teams have the skilled talent to effectively manage the industrial base and the supply chain to maximize competition, product choice, and negotiating leverage to maintain a healthy industrial base."* – DATS
>
> *"[T]he Department will ensure PAEs are empowered to manage their portfolio and deliver results through direct supervisory authority over professionals across critical disciplines, including acquisition, contracting, testing, and systems engineering. The OUSW(A&S) will establish accountability measures of merit that prioritize outcomes rather than activity across the acquisition enterprise. This will be addressed more extensively in the Acquisition Workforce Transformation Plan, prepared and delivered separately."* – DATS

In addition to Contracting Officers (KOs) and Contract Specialists, acquisition security professionals are an essential ingredient for success. As described in section G.2 of the unpublished DODI 5200.FH,[159] an acquisition security professional would be "[a]n Office of Personnel Management Security Administration Series General Schedule 0080 or equivalent position with a broad understanding of security countermeasures, risk mitigation strategies, and program and technology protection to assist in developing S&T [science and technology] and program protection planning." Additionally, section 3.2 of that same unpublished draft DODI, states acquisition security professionals, "[a]s security subject-matter experts who contribute to acquisition security integration throughout the DAS [Defense Acquisition System-recently renamed to Warfighting Acquisition System (WAS)]" would:

- "Meet requirements of an acquisition security training and credentialing program developed in accordance with DODM 3305.13 and the guidance in this issuance."
- "Support acquisition by helping to identify threats to emerging technology to enable rapid, uncompromised delivery of capabilities to the warfighter."
- "Consider information being released in open-source solicitation processes to prevent exposing critical information and operations."
- "Plan for how systems will be deployed, operated, maintained, and redeployed after fielding to ensure any reliance on commercial capabilities, infrastructure, services, or associated personnel is threat-informed. Develops security requirements that include defining security controls, developing security plans, and ensuring that security considerations are included in the design, development, and testing of systems."
- "Conduct security reviews of contracts, agreements, and other acquisition-related documents to ensure that they meet the required security standards. This includes reviewing contractor security plans, conducting vulnerability assessments, and ensuring that security controls are implemented and effective."

[159] OUSW(I&S) (Unpublished). *DOD Instruction 5200.FH: Acquisition Security [Draft].* Source: Unpublished draft policy.



- “Provide security training and awareness to program managers, contractors, and other stakeholders to ensure that they understand the security risks associated with the acquisition process and the steps that can be taken to mitigate those risks.”

There are a number of ways to foster stronger security awareness and management at all acquisition stages including:

- **Training and Education:** Programs like CDSE’s ED513[160] and cybersecurity courses build foundational knowledge for acquisition, security, and program professionals.
- **Security Toolkits and Reference Materials:** Use toolkits (e.g., CDSE Acquisition Toolkit[161]) and guidebooks to reinforce best practices.
- **Role-Based Integration:** Assigning dedicated security professionals and acquisition security professionals to acquisition teams supports continuous oversight and advocacy for security throughout the process and prevents potential oversights early in the process.
- **Routine Security Reviews:** Hosting tabletop exercises (e.g., DOD Cybersecurity Tabletop Guide[162]) and risk assessments during critical acquisition milestones ensures vulnerabilities are regularly evaluated and mitigated.
- **Collaborative Culture:** Encourage cross-functional communication between contracting, technical, and security experts to embed security considerations and promptly address evolving threats.

Integrating Security Throughout the Acquisition Process

Security must be a foundational element, integrated at every stage of the defense acquisition lifecycle—from planning and requirements determination to system retirement. Multiple sources, including oversight and statutory, reinforce this need for security collaboration across acquisition phases:

- FAR Part 7 Acquisition Planning[163] requires these security considerations:
    1. “For acquisitions dealing with classified matters, discuss how adequate security will be established, maintained, and monitored (see subpart 4.4).”
    2. “For information technology acquisitions, discuss how agency information security requirements will be met.”
    3. “For acquisitions requiring routine contractor physical access to a Federally-controlled facility and/or routine access to a Federally-controlled information system, discuss how agency requirements for personal identity verification of contractors will be met (see subpart 4.13).”

[160] CDSE (n.d.). *Security in the DOD Acquisition Process (ED513.10*). Source: https://www.cdse.edu/Training/Virtual-Instructor-led-Courses/ED513/

[161] CDSE (n.d.). *Acquisition Toolkit*. Source: https://www.cdse.edu/Training/Toolkits/Acquisition-Toolkit/

[162] DOD (2021). *Department of Defense Cyber Table Top Guide.* Source: https://www.cto.mil/wp-content/uploads/2023/06/DOD-Cyber-Table-Top-Guide-v2-2021.pdf

[163] GSA (n.d.). *FAR Part 7 - Acquisition Planning*. Source: https://www.acquisition.gov/far/part-7

4. “For acquisitions that may require Federal contract information to reside in or transit through contractor information systems, discuss compliance with subpart 4.19.”

- DFARS 252.204-7012[164] and related cybersecurity clauses mandate continuous data safeguarding and incident reporting across contract performance.
- GAO IT Acquisition Oversight Report[165] as stated in the ExecutiveGov’s article:[166] **“**Of the 16 programs [from various agencies that were audited], seven were found to be facing significant cybersecurity and information privacy risks, which escalate over time as existing infrastructure age and cyber threats become more complex. Ten were also deemed to potentially jeopardize the agency’s mission should the acquisition not push through.”
- OUSW(A&S) Other Transactions Guide (OT Guide), page 9[167] of the planning section states “[a]dequate advance planning for both the award of an OT agreement and any expected follow-on award is an essential ingredient of a successful program. Early, continuous communication and collaboration among all cross-functional team members will enhance the likelihood of a successful project.” The planning section also states that “[i]n addition to the project manager, end user, and warranted AO [Agreement Officer], the agency needs to secure the early participation of subject-matter-experts on the cross-functional team, such as legal counsel, comptrollers, contract administrative support offices, pricing team, and small business representatives to advise on agreement terms and conditions.” As stated in that section “[e]ach subject-matter-expert brings value to the team.”

  This is true; however, the guide would be more impactful if it adds security subject-matter-experts and acquisition security professionals to that list of CFT members. Otherwise, the potential of the OT Guide’s suggested CFT roles may be diminished, especially considering that section also says the subject-matter-experts “[enable] the Government to understand and manage risks throughout the lifecycle of the OT agreement to protect the Government interests and meet end user needs without unduly burdening performers.”[167] This statement implicitly supports the need for acquisition security professionals and would be strengthened to better serve the CFT and OT process as well as resultant agreements by explicitly stating acquisition security professionals should be CFT members.

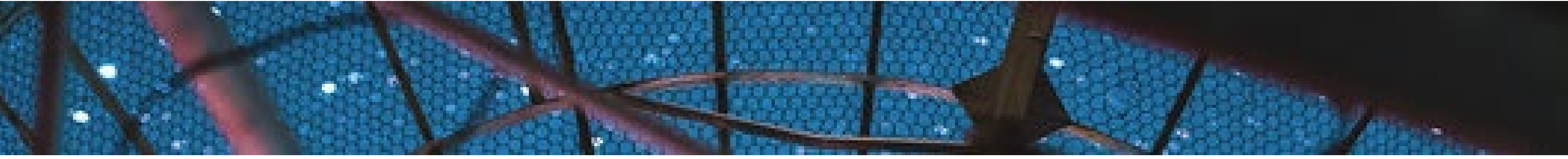
To improve the identification, inclusion, and execution of security requirements throughout the contract lifecycle (pre-award, post-award, close-out) the following are approaches, links to relevant sources and references, and successful agency examples. As the DATS may impact DOW’s current acquisition pathways or preferred acquisition methods, the guidance supported by the CDSE links may require revision, however, the fundamental security considerations should remain relevant. It is recommended that the CDSE resources be leveraged when revamping, revising, or drafting training or guidance pursuant to the DATS that impacts acquisition security.

[164] GSA (2024). *DFARS 48 C.F.R. § 252.204-7012. Safeguarding Covered Defense Information and Cyber Incident Reporting.* Source: https://www.acquisition.gov/dfars/252.204-7012-safeguarding-covered-defense-information-and-cyber-incident-reporting.

[165] GAO (2025). *Mission-Critical Information Technology: Agencies Are Monitoring Selected Acquisitions for Cybersecurity and Privacy Risks.* Source: https://www.gao.gov/products/gao-25-106908

[166] Jerry Petersen/ExecGov. (2025). *New GAO Report Tackles Risks and Challenges in Federal IT Acquisition Programs*. Source: https://www.executivegov.com/articles/gao-report-federal-it-acquisitions

[167] OUSD(A&S) (2023). *Other Transactions Guide July 2023*. Source: https://www.acq.osd.mil/asda/dpc/cp/policy/docs/guidebook/DoD%20OT%20Guide_July%202023.pdf



Integrating Security in Pre-Award Phase

> *"The inclusion of security SMEs [subject-matter-experts] during the requirements planning phase should result in a lower number of discrepancies in interpretation post-award. In general, Security SMEs seem to be resistant to new entrants. Perhaps this is due to the pace and level of technology being brought by new entrants.[...] I am sure you received feedback regarding the length of time DCSA is taking to get FOCI entities approved, as well as how long it takes to get FCLs and DD-254s in place. These processes seem to be long overdue for an overhaul."* – Industry interviewee

The recommendations herein support the inclusion of security SMEs, address new entrants to the DIB, and actions that can be taken during the pre-award phase to facilitate meeting security requirements.

1. Collaborative Requirement Development

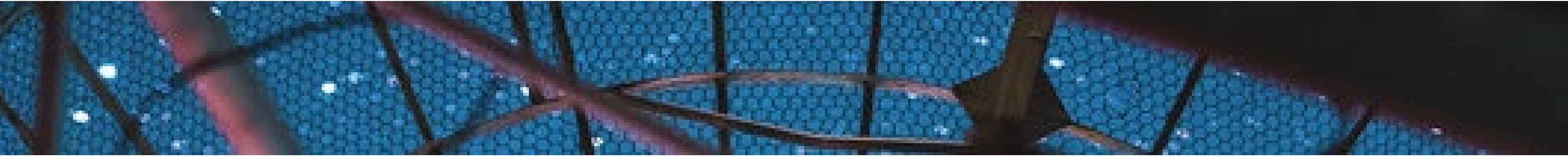
- Create CFTs and, if needed, integrated project teams (IPTs) with members from security, program, and contracting offices to validate and prioritize security requirements.[168]
- Leverage cross-functional/multidisciplinary teams (including program management, engineering, security, and acquisition/contracting), ensuring ongoing risk management and not just compliance.
- Require unified planning across security domains. During acquisition planning, security offices should work together along with acquisition security professionals as part of the CFT to assess risks, develop unified requirements, and draft or provide input into security language, as needed, that covers information, systems, personnel, and facilities.
- Integrate personnel, physical, and cybersecurity offices into requirements development, work statement, and solicitation drafting. Bring security experts into acquisition planning to review FAR, DFARS, and agency-specific clauses, and ensure proper handling of classified information via required forms such as DD-254 for any classified contracts.
- Define what requires protection, how much protection is necessary, and duration of protection. Proper classification guidance enables contractors to establish effective controls for Top Secret, Secret, or Confidential information. Guidance on how to do this within current acquisition pathways is available.[169]

2. Inclusion of Security Clauses

- Ensure all solicitations require compliance with mandated security frameworks (e.g., NISPOM for classified programs, DFARS for cybersecurity, Physical Security standards).

[168] DCSA (2024). *Acquisitions and Contracting Basics in the National Industrial Security Program (NISP), Version 4 Student Guide.* Source: https://www.cdse.edu/Portals/124/Documents/student-guides/IS123-guide.pdf

[169] DOD (2022). *DOD Directive 5000.01: The Defense Acquisition System*. Source: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/500001p.pdf



- Mandate use of DD-254 for classified contracts, specifying both contractor facility and personnel security requirements.[6]

3. Acquisition Strategy and Planning

FAR Part 7 and DFARS Part 207 require acquisition planning (e.g., Acquisition Strategy, Acquisition Plan, Industry Days, RFI). These start as soon as a need is identified, ensuring early risk management, including cybersecurity and supply chain threats.

- **Acquisition Strategy (Template/Form):** The Acquisition Strategy includes sections that address security and includes signature blocks that appear not to include security representatives. Adding signature blocks for the acquisition security professional and security organization(s) to concur or approve the Acquisition Strategy would encourage and reinforce the need for integrating security into the acquisition process.
- **Acquisition Plan (Template/Form):** The Acquisition Plan includes sections that address security and includes signature blocks that appear not to include security representatives. Adding signature blocks for the acquisition security professional and security organization(s) to concur or approve the Acquisition Plan would encourage and reinforce the need for integrating security into the acquisition process.
- **Industry Days:** Hold industry days or question and answer sessions that include federal and industry security experts to ensure security requirements are properly included in acquisition documents.
- **RFI:** Issue RFIs to request input on security requirements and performance measures to ensure they are properly included in acquisition documents.

4. Proposal Evaluation

Incorporate non-price factors into the evaluation that encourage new entrants and smaller businesses, and foster security planning. Clearly specify how these factors will be evaluated (e.g., using color/adjectival or confidence ratings). Tailor security evaluation criteria to program risk and risk tolerance; lower-risk tolerance contracts may require more detailed and specific factors.

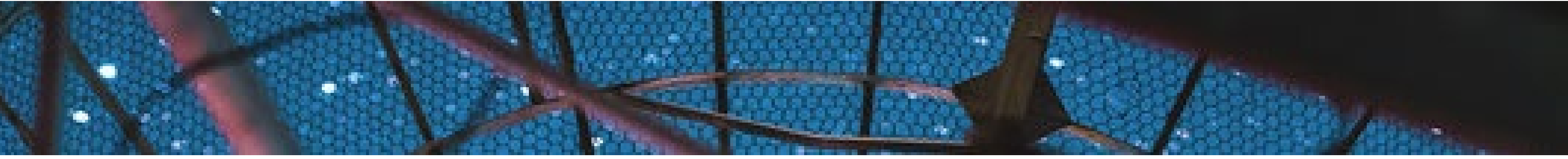
- **Experience of contractors:** This would entail the offeror explaining how they would apply their *experience* in XYZ technical and/or security requirements, supported by examples of that prior *experience*. Note: Before requiring experience examples in a particular area, carefully consider how this might impact companies with little to no experience in such an area, especially when seeking to encourage new entrants. An experience factor or criterion could be written in a manner that allows offerors to include examples of corporate, federal, state or local government experience (not just DOW). The number of examples required from whom (prime, subcontractor or both) and in what role (prime or subcontractor) must be made very clear in the instructions to offerors and in the evaluation factors/criteria. When considering the use of experience, it may be helpful to request references for that experience. Work closely with the KO before RFP release to strategize the best approach that would prevent unduly prolonging the evaluation process or introducing protest risk.

- **Past performance of contractors:** Before including past *performance* as an evaluation factor, consider if/how including past performance might unduly restrict competition or new entrants (unless technical requirements or security would otherwise be compromised). If past performance is evaluated, the solicitation:
    - Could require the past performance examples be for the same contracts referenced for the experience examples (if experience examples are requested). This encourages veracity in the experience examples.
    - Could allow past performance examples of corporate, federal, state, or local government *performance* (not just DOW).
    - Should specify if examples can be those of the proposed prime contractor, subcontractor, or both.
    - Should specify if examples can be for performance in the prime contractor or subcontractor role.
- Indicate Contractor Performance Assessment Report System (CPARs) and other reporting systems may be checked to validate proposal experience and past performance examples.
- Identify qualifications and certifications of key personnel in security roles.
- Describe technical (or management) approach to maintaining security, incident response, and reporting.

The remainder of this pre-award section provides potential proposal evaluation factors and criteria that may alleviate barriers to entry. They are not all inclusive or relevant to all acquisitions. This section also provides potential proposal evaluation factors and criteria that highlight security in an effort to ensure security is adequately addressed throughout the acquisition lifecycle. The examples are intended to spark ideas among the government stakeholders who would draft the proposal evaluation criteria for acquisitions they pursue. It is important to consider if such types of factors/criteria are relevant to a particular acquisition and beneficial to evaluate. If they are relevant and beneficial, they should be tailored to the respective acquisition.

Innovation Factors/Criteria: Including innovation as an evaluation factor/criteria may encourage innovators/companies to submit a proposal if innovation will be a factor/criterion that the government evaluates to select the contract awardee. It may also encourage larger or more traditional companies to team with innovators, opening doors for such companies and innovators.

The core concept is that contractors are assessed on their ability to demonstrate “innovation” through proposed changes or improvements, as outlined in their proposals, that have a quantifiable impact on cost, schedule, or performance. This approach ensures that innovation is not merely a marketing statement or a series of broad promises but rather a measurable and tangible factor. A critical aspect of this process is clearly communicating in the RFP and accompanying instructions that the Government reserves the right to incorporate any proposed innovations into the resulting contract award. This ensures that contractors are held accountable for delivering on the innovative solutions they propose during contract execution. Additionally, quantifiable savings or innovations supported by hard data make it challenging for other companies to lodge protests, thereby enhancing the integrity and fairness of the evaluation process.



Innovation needs to be defined in any solicitation using innovation as a factor to ensure 1) offerors understand what is considered innovation so that offerors propose accordingly, and 2) the proposal evaluation team understands what to evaluate the proposals against so that the proposals are consistently and fairly evaluated.

Example Definitions of Innovation and Novelty

Innovation as it applies to this solicitation is defined as the combination of novel, executable approaches to meet or exceed government requirements and deliver impact to the government.

Novelty alone, without impact, will not be considered true innovation.

Novelty is defined as the introduction of new or transformative tools, technologies, methods, or processes. Impact is defined as the ability to solve problems or drive meaningful positive change, such as improving efficiency, saving lives, reducing costs, or enabling transformation.

Examples:

- "The proposal will be evaluated on the extent to which it demonstrates an innovative <<e.g., solution, solutions, technical approach>>."
- "The proposal will be evaluated on the extent to which it demonstrates an innovative <<e.g., solution, solutions, technical approach>> to <<insert a particular aspect that the government wants to hone in on; something it deems would be critical to the likelihood of successful performance or outcomes>>."
- "The proposal will be evaluated on the extent to which it demonstrates the incorporation of innovative <<e.g., solution, solutions, technical approach>>."
- "Proposals should demonstrate how the proposed <<e.g., solution, solutions, technical approach>> is innovative - combines novelty with measurable impact."

Security Approach Factors/Criteria: Including security evaluation factors/criteria requires offerors to address security in their proposals so that the evaluation team can evaluate their likelihood to successfully meet security requirements. It also opens a crosswalk (later in the source selection process) to the price proposal to ensure the offerors' "technical approach" to security is commensurate to their proposed price. Security related evaluation factors, subfactors, or criteria may include elements such as:

- Technical approach to security (cyber/physical/personnel), including compliance plans.
- Qualifications and certifications of key personnel in security roles.
- Management approach to maintaining security, incident response, and reporting.

It is necessary to tailor security evaluation criteria to program risk. Higher-risk contracts may require more detailed and specific factors depending on the level of risk the government is willing to take. This does not mean waiving required security compliance. Instead, it means the evaluation team may require offerors to provide more detailed information on areas that have a higher likelihood to introduce risk or impact the success of the contract and supporting mission needs. As DATS is moving toward becoming less risk averse, it is critical that risk still be assessed so that the risk tolerance can be adequately determined.

Consider that security factors/criteria can be organized into a dedicated Security Volume, separate from the Technical Volume, allowing the government's security experts to focus specifically on security-related aspects. Regardless of whether security elements are included in the Technical Volume or a separate Security Volume, it is essential to ensure that neither the technical approach nor the security approach is evaluated in a vacuum. A crosswalk should be conducted to ensure the technical approach and the security approach effectively align for a successful solution.

Below is an extensive list of potential high-level security evaluation factors/criteria that could be incorporated into solicitations. These examples should be tailored and the order of importance specified to prioritize key factors that assess offerors' likelihood of successful performance and security compliance. Including all examples may unduly prolong the evaluation process. Therefore, the program, security, and acquisition offices should collaborate to ensure the evaluation factors (whether or not prompted by the examples) enable technical evaluators to select the contractor that overall will best meet the government's needs (in accordance with the RFP). When determining what elements are needed, consider the needs of national security, IT-intensive programs, and mission risk tolerance. Security factors/criteria can be categorized into physical, personnel, and cyber security. Treat physical, personnel, and cyber security as distinct technical evaluation elements (not just "compliance").

Examples:

- Offerors will be evaluated on whether the offeror (prime and proposed subcontractors) is certified at the requisite CMMC level. Note: This would likely be Pass/Fail and address which level is required for award. Instructions would describe what the offeror must provide to prove they meet the requisite CMMC maturity level.
- Offerors will be evaluated on their approach to security including the following:
    - Prime and proposed subcontractors' technical approach to meet subsequent CMMC phase(s) required levels.
    - Safeguarding Covered Defense Information and Cyber Incident Reporting Compliance to comply with DFARS 252.204-7012.[170]
    - Effectiveness of systems protection plan and continuous monitoring.
    - Effectiveness of Cybersecurity Incident Response Plan.
    - System Security Engineering (SSE) inclusion of mission-based cybersecurity risk assessments and threat intelligence integration.
    - Security architectures.

[170] GSA (2024). *DFARS 48 C.F.R. § 252.204-7012. Safeguarding Covered Defense Information and Cyber Incident Reporting.* Source: https://www.acquisition.gov/dfars/252.204-7012-safeguarding-covered-defense-information-and-cyber-incident-reporting.

    - Complete personnel security clearance paperwork in accordance with the timeframes described in the PWS.
- Offerors will be evaluated on how they will apply their experience in the following areas to effectively integrate and comply with security requirements to successfully deliver <<products, services>>.
    - Industrial Security to comply with DODM 5205.07 NISPOM requirement: This is broad and could be refined to discriminating factors or areas within DODM 5205.07 NISPOM of most concern or highest security risk and does not mean the awardee would not have to comply with the other DODM 5205.07 NISPOM requirements included in the solicitation and contract.
    - Cybersecurity Posture: Security architectures, vulnerability management, patch timelines, cyber insurance.
    - Personnel Security/Qualifications: Vetting, clearance status, continuous training.
    - Incident Response Maturity: Demonstrated ability to respond rapidly and thoroughly to breaches.
    - Physical Security Compliance: Facility safeguards, access control, surveillance practices.
    - Regulatory Compliance: Compliance history with <<e.g., DFARS 7012, NIST 800-171>>.

Illustrative Technical and Cost Proposal Evaluation Factors/Criteria:

Table 7 provides examples of instructions to offerors and evaluation criteria for three cybersecurity areas. The instructions column includes example instructions to offerors describing what their proposal must include regarding these three cybersecurity areas. The evaluation column provides examples of what to evaluate to ensure the government's requirements are met in these areas as well as to ensure the technical/security proposal aligns with the cost/price proposal. This table is illustrative, therefore, verbiage would require vetting, as described in the footnotes, to ensure the instructions and evaluation criteria that ultimately appear in a solicitation align with each other and are free from ambiguity.

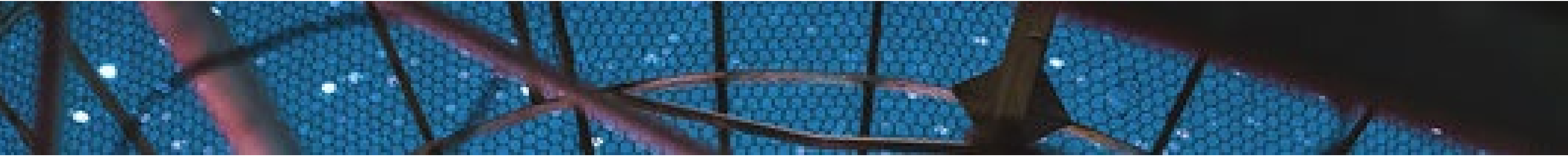
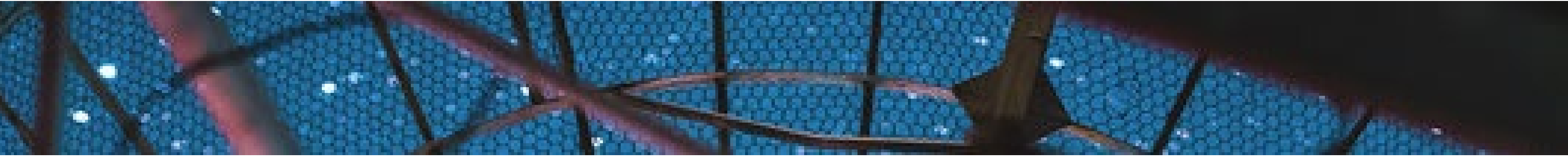


Table 7. Illustrative Cybersecurity Evaluation Criteria in Technical and Cost Volumes

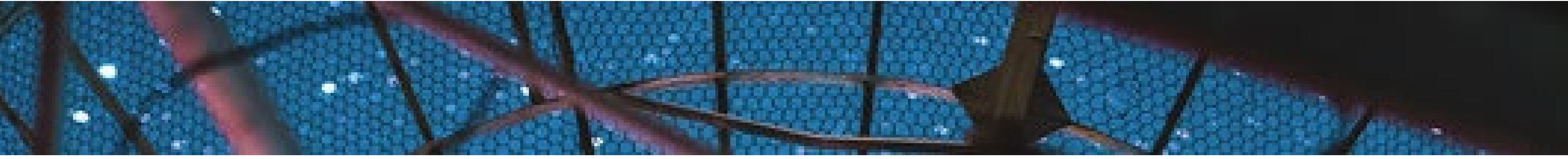
Area	Section L - Proposal Instructions[171]	Section M - Evaluation[172]
1. Cyber Trustworthy Software Bill of Materials (TSBOM)	Offerors shall demonstrate their capability to produce, maintain, and operationalize a Trustworthy Software Bill of Materials (TSBOM) across the system lifecycle. At a minimum, the proposal shall include: (1) a representative TSBOM artifact in an industry-recognized format (e.g., SPDX, CycloneDX) aligned with NTIA guidance; (2) identification of all software components, direct and transitive dependencies, versions, and known vulnerabilities; (3) description of TSBOM generation, update cadence, and validation at build-time and during sustainment; (4) explanation of how TSBOM data supports vulnerability management and risk-informed decisions; (5) approach for handling proprietary or opaque components; and (6) a cost cross-walk covering TSBOM tooling, labor, sustainment, and updates.	The Government will evaluate the extent to which the offeror provides a complete and standards-aligned TSBOM; sustains TSBOM accuracy over time; integrates TSBOM data into operational vulnerability management rather than treating it as a static artifact; and accounts for all costs required to implement and sustain the proposed TSBOM capability without omissions affecting cost, schedule, or performance.
2. Telemetry Implementation and Integration	Offerors shall demonstrate how telemetry capabilities are implemented and used as an operational control to support system performance, cybersecurity, and authorization sustainment. At a minimum, the proposal shall include: (1) a telemetry architecture identifying data sources, collection mechanisms, storage, retention, and analysis; (2) identification of decision authorities who consume telemetry and actions enabled by that data; (3) examples of telemetry supporting continuous monitoring, incident detection and response, and performance management; and (4) a cost cross-walk for telemetry tools, licenses, infrastructure, labor, and sustainment.	The Government will evaluate whether the telemetry approach enables timely detection and response; produces actionable data rather than passive logs; scales across the system lifecycle; and is fully supported by the proposed cost/price.
3. Zero Trust (ZT) and Endpoint Detection and Response (EDR)	Offerors shall demonstrate how Zero Trust principles and EDR capabilities are integrated into the system architecture to reduce attack surface and support continuous risk management. At a minimum, the proposal shall include: (1) alignment to DOW Zero Trust pillars and maturity expectations; (2) description of integrated identity, access control, device posture, and monitoring; (3) explanation of how EDR supports detection,	The Government will evaluate the extent to which the offeror demonstrates a coherent Zero Trust architecture rather than a collection of tools; shows measurable improvements in detection, containment, and response; and aligns

[171] The "Section L – Proposal Instructions" column includes example instructions to offerors describing what their proposal must include regarding these three cybersecurity areas. The "cost driver" text may require refinement, and the respective technical/security and cost/price evaluation criteria would need to clearly align with the instructions.

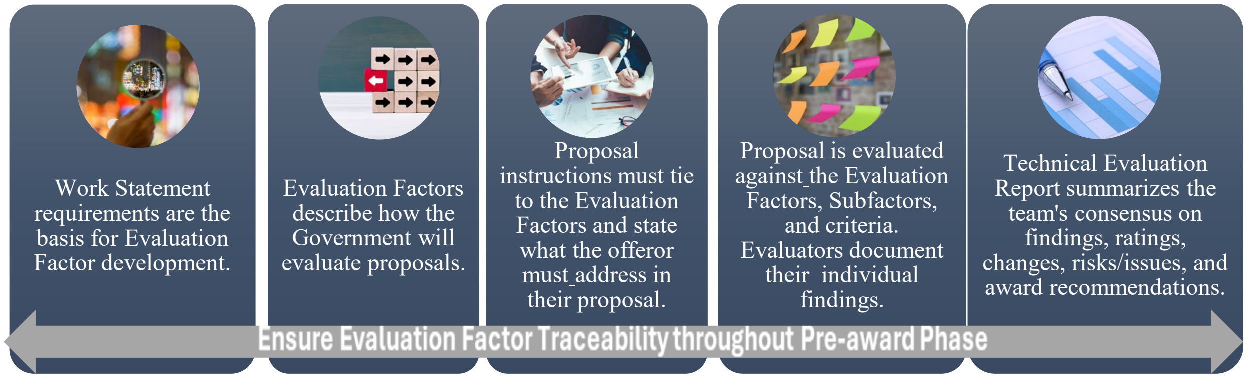
[172] The "Section M – Evaluation" column addresses cybersecurity-area elements and cost/price elements; aiming to provide examples of what to evaluate to ensure the government's requirements are met and to ensure the technical/security proposal aligns with the cost/price proposal. The cybersecurity approach to these areas and their cost/price elements would each need to be placed in their respective areas of Section M. (i.e., technical/cybersecurity elements go into the technical/security volume of the proposal and cost/price goes into the cost/price volume of the proposal). When the evaluation criteria are written, the instructions must be written to clearly align with the evaluation criteria.



Area	Section L - Proposal Instructions[171]	Section M - Evaluation[172]
	response, and recovery; (4) identification of inheritance strategies and shared services; and (5) a cost cross-walk for implementation, integration, licensing, and sustainment.	technical claims with realistic and complete cost assumptions.
4. Authorization Readiness and Cyber Evidence Sustainment	Offerors shall demonstrate how cybersecurity artifacts and operational data are produced and maintained to support initial authorization and ongoing authorization readiness. At minimum, the proposal shall include: (1) description of how authorization-relevant cyber evidence is generated, maintained, and reused; (2) explanation of how telemetry, TSBOM, and Zero Trust artifacts support ongoing authorization decisions and reciprocity; and (3) identification of roles responsible for maintaining authorization evidence.	The Government will evaluate whether the offeror demonstrates a credible approach to sustaining authorization-relevant cyber evidence; enables reuse of evidence and minimizes rework; and reduces the risk of authorization delays caused by incomplete or inconsistent cyber artifacts.
5. Vulnerability Response and Compensating Controls	Offerors shall describe how vulnerabilities are prioritized, mitigated, and managed when standard remediation is not feasible due to operational, vendor, or architectural constraints. At a minimum, the proposal shall include: (1) approach to vulnerability prioritization and risk-based decision making; (2) use of compensating controls when patching is not possible; and (3) expected mitigation timelines based on severity and mission impact.	The Government will evaluate the extent to which the offeror demonstrates realistic, risk-informed vulnerability response processes; accounts for operational constraints; and provides credible mitigation strategies rather than assuming ideal remediation conditions.
6. Cyber Sustainment and Cost Realism	Offerors shall describe how cybersecurity capabilities will be sustained over the life of the system. At a minimum, the proposal shall include: (1) identification of cybersecurity capabilities requiring ongoing sustainment; (2) description of cost drivers such as licensing growth, labor, and infrastructure; and (3) assumptions regarding government-furnished or shared services.	The Government will evaluate whether the offeror presents realistic sustainment assumptions; clearly identifies long-term cybersecurity cost drivers; and avoids omissions that could result in degraded cybersecurity posture over time.
7. Integration of Cybersecurity into Program Execution	Offerors shall describe how cybersecurity considerations are integrated into system engineering, development, operations, and program management. At a minimum, the proposal shall include: (1) examples of program decisions informed by cybersecurity considerations; and (2) identification of roles responsible for cyber-related tradeoffs affecting architecture, schedule, or performance.	The Government will evaluate the extent to which the offeror integrates cybersecurity into overall program execution rather than isolating it; and demonstrates clear ownership and accountability for cyber-related decisions.



Trace evaluation factors throughout pre-award documents: Traceability of evaluation factors throughout the pre-award phase is critical and ultimately impacts contract performance. When Evaluation Factors are fully drafted, review the Work Statement to ensure each factor correlates to text in the Work Statement. Double check this before submitting the acquisition package to the acquisition office and again when reviewing the solicitation before its release. This reduces protest risk AND provides another opportunity to ensure security related requirements are appropriately addressed in the Work Statement so that such requirements are included in the resultant contract. Doing so also affords opportunity to ensure the selected offeror addresses security in their proposal to the extent necessary to increase the likelihood of post-award compliance. Figure 9 demonstrates the relationship of evaluation factors to various acquisitions documents and acquisition phases.



Work Statement requirements are the basis for Evaluation Factor development.

Evaluation Factors describe how the Government will evaluate proposals.

Proposal instructions must tie to the Evaluation Factors and state what the offeror must address in their proposal.

Proposal is evaluated against the Evaluation Factors, Subfactors, and criteria. Evaluators document their individual findings.

Technical Evaluation Report summarizes the team's consensus on findings, ratings, changes, risks/issues, and award recommendations.

Ensure Evaluation Factor Traceability throughout Pre-award Phase

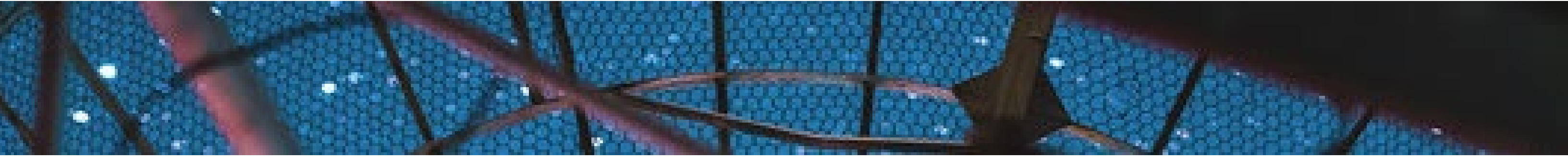
Figure 9. Example Evaluation Factor Traceability

Integrating Security in Post-Award Phase

1. Formal Performance Measures and SLAs

Security performance measures can help monitor contract performance while also incentivizing contractors to prioritize security. By doing so, contractors can achieve favorable outcomes such as enhanced resilience against security threats and increased competitiveness for future contracts. Contractors may also be incentivized to further invest in their company’s security awareness or security infrastructure if they are rewarded for it. Emphasizing and investing in security can help mitigate or prevent risks such as data breaches, intellectual property theft, operational disruptions, and non-compliance, thereby minimizing the likelihood of low CPARS ratings.

This section outlines potential performance measures that may be used post-award to assess the effectiveness of the contractor's execution. These measures are not exhaustive nor applicable to all acquisitions but are intended to inspire ideas among government stakeholders responsible for defining performance metrics for their specific projects. It is important to determine whether these measures are relevant and beneficial for a particular acquisition. If deemed appropriate, they should be customized to align with the unique objectives and requirements of the acquisition. The performance measures can be included in the PWS, addressed in Quality Assurance Surveillance Plans, Quality Plans, or other related documents. Including the performance measures in RFIs for industry feedback, and requesting suggested performance measures from industry during the RFI process, enables the government to include measures that are both impactful and effective.



Post-Award Case Studies: Security Successes: *DOW GBSD Program*

By embedding the Cyber Resiliency Office for Weapon Systems (CROWS) and Mission Defense Operations Center (MDOC) into acquisition planning, source selection, and system engineering, GBSD improved program resilience and reduced cybersecurity risk exposure in post-award operations.[173]

Examples:

- Include Service Level Agreements (SLAs) that set quantifiable thresholds for security; e.g., percentage of vulnerabilities remediated within timeframe, background check completion rates, physical access control compliance. An INSA whitepaper[174] addresses considerations that inform writing SLAs. While dated April 2017, the whitepaper still makes points that are relevant today including those for the outcome-based acquisition, as emphasized in the DATS.
- Define how metrics will be monitored (e.g., audits, continuous monitoring, physical inspections, vulnerability scans) and enforced (penalties, service credits, corrective action plans) or rewarded (especially when an incentive type contract). As an incentive for continued compliance, the contract should indicate the government will monitor adherence to security requirements, metrics and SLAs and record positive and negative performance in CPARS. This may resonate with industry as CPARS ratings could have an impact on their past performance ratings in future source selections. Table 8 provides example sample performance measures.
- Structure performance measures/evaluations around key milestones and contract closeout, documenting contractor performance on security.[175]

Table 8. Sample Performance Measures

Metric/Criteria Category	Example Threshold	Surveillance Method	Enforcement/ Impact
Cybersecurity Vulnerability Remediation	X% remediated within X days	Audit, report review	Service credits, penalties, CPARs
Personnel Clearance Processing	X% cleared before start	Clearance database checks	Withhold access, breach, CPARS
Personnel Clearance Processing	Within X days of contract start date, submit clearance paperwork for X% of proposed staff.	Clearance database checks	CPARS

[173] DOD (2021). *Cybersecurity for DOD Acquisition Program Execution: Best Practices for the Major Capability Acquisition Pathway Insights from the Ground Based Strategic Deterrence (GBSD) Program*. Source: https://www.acq.osd.mil/asda/pwpm/docs/dau/Cybersecurity_Best_Practice_Guidebook_Version_1-24Nov2021.pdf Cybersecurity_Best_Practice_Guidebook_Version_1-24Nov2021.pdf

[174] INSA (2017). *Improving Acquisition Of Services In The Intelligence Community*. Source: https://www.insaonline.org/docs/default-source/uploadedfiles/2017/12/insa-improving-acquisition-april-2017.pdf

[175] DOD (2025). *Management Advisory: Timeliness of Performance Evaluations for Contracts Supporting the DOD's Building Partner Capacity Efforts (Report No. DODIG-2025-080).* Source: https://media.defense.gov/2025/Apr/01/2003679045/-1/-1/1/DODIG-2025-080_REDACTED_SECURE.PDF

Personnel Clearance Timely Response	X% of Contractor staff per X months complete and submit their security paperwork/form within X days of receiving a notice to complete security paperwork X	Clearance database checks	CPARS
Physical Security Compliance	X% compliance reviews passed	On-site inspections	Corrective actions, CPARS
Incident Reporting Timeliness	X% within X hours (Response times would be tailored to the type and levels of incidents)	Incident log review	Contractual penalties, CPARS
Cyber Incident Response	Mean Time to Detect and Recover ≤ X hours	Incident log report vs. baseline	CPARS
Vulnerability Management	% of critical patches applied within X days	Security audit data	CPARS
Security Training	% of cleared staff with annual training updated	Personnel security records	CPARS
Data Protection	Zero critical data leaks per quarter	Compliance audit	CPARS

Integrating security into performance measures protects programs from costly vulnerabilities. Prioritizing CMMC-aligned cybersecurity resilience, SCRM, and quantifiable post-award metrics—reinforced by DFARS requirements and security-linked incentives—transforms compliance into strategic value.

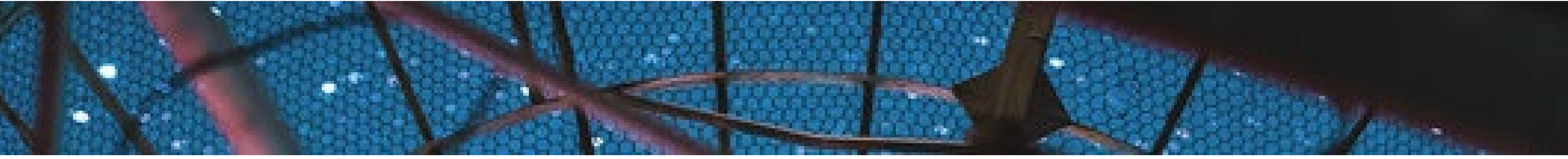
2. Program Offices Holding Contractors Accountable

Program managers and contracting officer representatives (CORs) should be provided with acquisition security professional support and CDSE training. The professionals and training will help the COR with post-award oversight responsibilities, such as periodic reviews and compliance checks on security requirements like clearances, storage protocols, and clause adherence. Collectively, these actions support the President's Management Agenda[176] goal to build the most agile, effective, and efficient procurement system while ensuring accountability for results—including security.

Examples:

- Require regular reporting and deliverables on compliance (security posture reports, incident logs, personnel clearance status).
- Schedule and document regular compliance reviews, penetration tests, and site visits.
- Establish clear escalation paths for reporting and remediating non-compliance.

[176] Executive Office of the President (2025). *President's Management Agenda*. Source: https://www.performance.gov/pma/



3. Integrated Oversight and Communication

It is critical that the government maintain active communication and information-sharing between program, security, and contracting offices during contract execution. They can utilize contract management tools to track compliance with security requirements across all stakeholders, and consider integrating tools if feasible and cost efficient.

4. Subcontractor Management

Ensure prime contractors flow all required security clauses down to subcontractors and check that subcontractors comply, including reporting and controls for classified work or CUI.[177] The text in some security-related FAR and DFARS clauses already require these flowdowns, but does not address how which leads to variance. For example, as shown in Appendix C, some clauses require the flowdown to be substantially the same, to use similar language, or to use the same clause verbatim. The clauses that afford the prime contractor some flexibility in what the flowdown text should say, opens a door to ensure the prime contractor flows down what is germane to the subcontractor's performance. It also opens the door for interpretation on what is considered substantially the same or similar. This could introduce risk to the government, the prime or the subcontractor. As such, it is suggested that offerors be required to indicate their procedures for ensuring subcontractor compliance to security requirements to include any flowdown of clauses.

Integrating Security in Close-Out Phase

- **Contract Close-out Requirements:** Follow current close-out requirements and reference DOD's 2019 Contract Closeout Guide Book,[178] or revise it if needed to implement DATS. Requirements from the Contract Closeout Guidebook include:
    1. Security Requirements Checklist: Utilize comprehensive contract close-out checklists, such as DD Form 1597, to verify disposition of classified material, patents, royalties, and proper reporting (e.g., final reports in eSRS for subcontracting plans).
    2. Disposition of Sensitive Material: Confirm through DCSA or equivalent that all classified or sensitive data and materials have been disposed of, and annotate this before official contract closure.
    3. System Access Termination: Close or retire any government system access codes (like DODAAC) given to contractors, ensuring that no further access is possible after contract end.
- **Contract Close-out PWS Requirements:** Include requirements as needed in the PWS to ensure that the contractor is aware of and bound to its contract close-out requirements.
- **Lessons Learned Sharing:** Conduct lessons learned involving acquisition/contracting offices, security offices, and program offices to improve future contract security integration or close-out and update processes, approaches, and DOD's Contract Closeout Guide Book accordingly.

[177] Hunton Andrews Kurth LLP (2025). *New Cybersecurity Requirements for Federal Contractors.* Source: https://www.hunton.com/privacy-and-information-security-law/new-cybersecurity-requirements-for-federal-contractors

[178] DOD (2019). *Contract Close Out Guidebook*. Source: https://dodprocurementtoolbox.com/uploads/Contract_Closeout_Guidebook_20191025_Final_5ed6c5333f.pdf

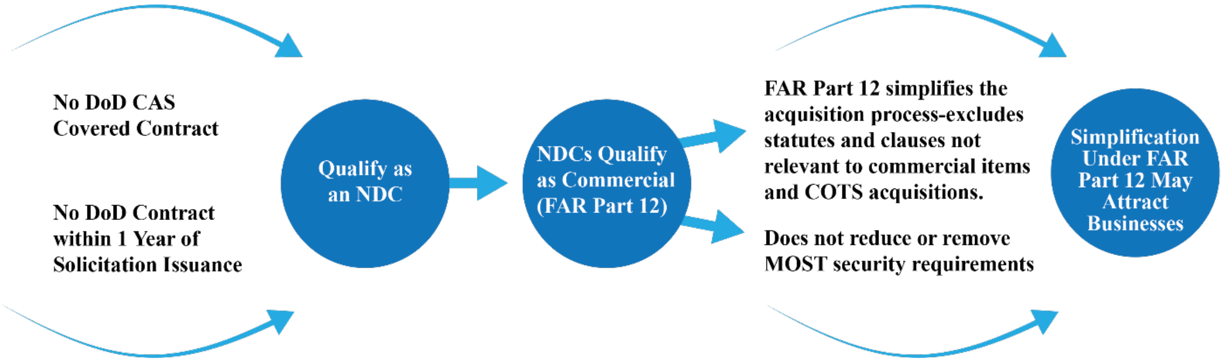
ADVANCING INNOVATION IN DOW ACQUISITIONS

Overview of stakeholders, organizations, partnerships, opportunities and methods available to advance innovation within DOW

- **DOW Acquisition and Program Offices**
  - Defense Innovation Unit (DIU): Accelerates commercial tech adoption for national security by coordinating prototyping and field deployments.
- **Industry Engagement Organizations**
  - Consortium for Command, Control, and Communications in Cyberspace (C5): Rapid, cost-effective acquisition for information technology innovators (including SMBs and NDCs).
  - Mentor-Protégé program: Partners small businesses with established DOW contractors to develop business and cleared facility capabilities.
- **Public-Private Partnerships and Support Channels**
  - General Services Administration (GSA): Provides secure workspace and SCIF leasing solutions to contractors—including collaborative and co-working models.
  - SBIR/STTR programs: Offer R&D funding, support infrastructure, and commercialization opportunities for small businesses and academic partners.
  - Acquisition Innovation Research Center (AIRC): This applied academic research arm of DOW partners with over 25 universities to connect acquisition experts with faculty and students, translating research into practical applications to meet Warfighter needs.
- **Commercial Facility and Security Service Providers**
  - Classified Infrastructure-as-a-Service companies: Lower barriers to facility clearance and classified workspace for small, innovative contractors in major defense regions.
- **Opportunities**
  - Engage consortiums (DIU, C5, NAC, NSIN) for rapid tech onboarding, joint problem-solving, and sharing facility/security resources.
  - Leverage government-backed programs (SBIR/STTR, Mentor-Protégé, GSA) to strengthen infrastructure, mentor partnerships, and compliance knowledge.
  - Integrate local, regional, academic, and nonprofit entities to enhance innovation pipelines and provide near-market support.

Streamlined Pathways for Participation

As it can be difficult for small businesses and NDCs to access DOW contracts and comply with DOW and federal regulations, *qualifying* as an NDC as described herein opens the door to industry for their products or services to be deemed as commercial and eligible to be procured under FAR Part 12. Embracing this contracting approach could decrease industry hesitancy to submit proposals and remove real or perceived barriers to entering the DIB, thus closing innovation gaps and increasing the variety or representation of companies within the DIB. (e.g., more companies, particularly small businesses, startups, or NDCs). Figure 10 demonstrates how contractors can “qualify” as an NDC and then “qualify” as commercial which allows for more streamlined acquisition to attract companies into the DIB.


No DoD CAS Covered Contract
No DoD Contract within 1 Year of Solicitation Issuance
Qualify as an NDC
NDCs Qualify as Commercial (FAR Part 12)
FAR Part 12 simplifies the acquisition process-excludes statutes and clauses not relevant to commercial items and COTS acquisitions.
Does not reduce or remove MOST security requirements
Simplification Under FAR Part 12 May Attract Businesses

Be strategic: attract NDCs by highlighting the advantages of commerciality, optimize the contract period of performance during which the company qualifies as commercial as an NDC, and evaluate potential security impacts.

Figure 10. Attract and Ameliorate Access to the DIB

The following are FAR Part 12 attributes and notable areas to navigate strategizing its use for NDCs.

- Streamlining Focus: FAR Part 12 simplifies the acquisition process by excluding statutes and clauses that are not relevant to commercial items and COTS acquisitions.
- Mandatory Clauses: Only a few key clauses are required, and additional clauses are strongly restricted. FAR Subpart 12.5 (12.503–12.505) identifies statutes and clauses that do not apply to commercial item acquisitions.
- Executive Order 14265: “Modernizing Defense Acquisitions and Spurring Innovation in the Defense Industrial Base”[179] encourages the use of commercial contracts.

Pursuing this approach should be done strategically because when the NDC begins supporting DOW (e.g., awarded and performing work), they would no longer be eligible to be considered an NDC (and commercial) when pursuing other DOW contracts (unless commercial in and of

[179] The White House (2025). *Modernizing Defense Acquisitions and Spurring Innovation in the Defense Industrial Base.* Source: https://www.whitehouse.gov/presidential-actions/2025/04/modernizing-defense-acquisitions-and-spurring-innovation-in-the-defense-industrial-base/

themselves, not because of the NDC determination). The DATS strongly encourages the use of commercial products and services. Below are high level considerations to strategically procure services from NDCs on a commercial basis.

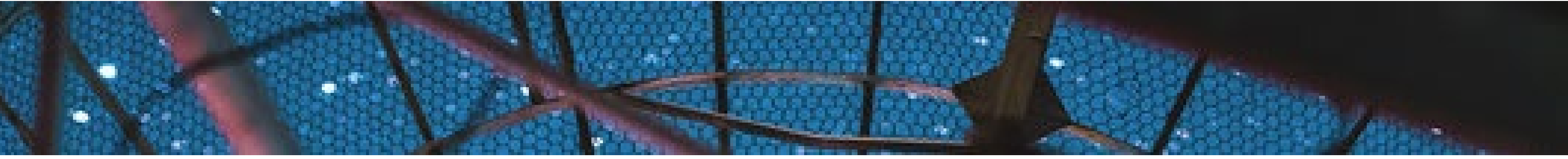
Advantages to contractors due to exclusion of clauses: Reduced compliance burdens, fewer reporting requirements, and lower audit exposure. FAR Subpart 12.5 (12.503–12.505) identifies statutes and clauses that do not apply to commercial item acquisitions.

When an interviewee was specifically asked “If government/companies were to use FAR Part 12, do you foresee any shortfalls that would impact security or industry’s ability to meet government security requirements?” The response was “*No, given the regulatory requirements pertaining to security still apply when the USG procures commercial products and/or services (e.g., CMMC 2.0. NIST 800-171, DFAR 252.204-7008/7009/7012, etc.). The pain-point is the $$$$ required for compliance. The USG should consider implementation costs to comply with these requirements as an allowable cost to USG projects as well as consider a systematic, phased, approach for compliance. It doesn't make sense that a Small Business winning a $100,000 study contract should be required to spend $50-$60K to obtain third-party validation of its CMMC compliance.”*

Contract Duration and Funding: If the contractor is considered commercial by virtue of being an NDC, explore the use of multi-year base periods to alleviate contractor hesitation to pursue contracts that require investments in secure facilities and mature security practices. As the initial period of performance for a multi-year base period would be longer than the traditional 12-month base period, such a duration may potentially provide potential NDCs or small business offerors a higher level of confidence of continued performance and funding, thus potentially reducing risks to a return-on-investment.

As a point of clarification, multiple year and multi-year contracts sound similar but they mean two different things in the FAR/DFARS context. A multiple year contract (which is most typical and sometimes called a "base plus options" contract) covers more than one year, but each additional year is exercised separately as an option. (For example: a 5-year period of performance with one 12-month base period and four 12-month *option* periods. Or, 3-year period of performance with one 12-month base period and two 12-month *option* periods, etc.) A multi-year contract on the other hand is a contracting method that would allow the government to “buy more than one year's requirement (supplies or services.)” (For example: if the government requires three years of work (supplies or services) “all at once” they could use a 3-year base period vs the more traditional one 12-month base period with two 12-month option periods). The government must be able to justify a multi-year contract approach and have the type of funding to do so.

Establishing multi-year base periods may alleviate contractor hesitation to pursue contracts as the initial period of performance would be longer than the traditional 12-month base period. Funds (provided they are available and the correct type) may be obligated upfront during the multi-year period versus waiting for annual option years to be exercised to authorize and fund continued performance. NDCs may be inclined to pursue multi-year contracts (longer base periods of performance) if they perceive that as a way to mitigate risks of (1) Investing in facilities and



attaining and maintaining certifications such as CMMC and (2) Navigating delays in on-ramping due to personnel and facility clearances

While contracts can go beyond five years, some KOs or organizations could be reluctant to take the longer duration contract route to avoid potential “vendor lock-in”, limiting competition, or potentially limiting the opportunity to access innovative or emerging technologies. The use of a multi-year contract or a contract with a period of performance exceeding five years must be justified and approved by the KO (and in some cases above the level of the KO) prior to solicitation release. Security, complexity of the requirement and the program requirements may all factor into the justification. Note: Multi-year contract periods can be used under FAR Part 12/commercial contracting as well as non-commercial contracts. In either scenario, the government always reserves the right to terminate contracts for convenience. So, a multi-year contract is not an iron clad guarantee for continued performance. The use of a multi-year contract must be justified and approved by the KO. Security, complexity of the requirements, and program requirements may all factor into the justification.

Use for classified contracts: While the use of Commercial, FAR Part 12, contracts may encourage NDCs to work with the DOW, costs to support classified contracts may deter the NDCs. To address that, the contract could be planned and structured to ensure only unclassified work is required while the contractor works toward gaining the requisite facility and personnel clearances or SCIF access.

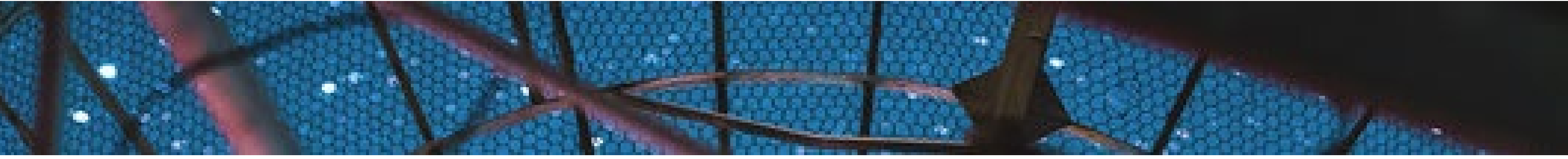
An interviewee was asked if they had seen any good examples of the government up-front (e.g., FAR Part 12) providing graduated milestones for security for work that was anticipated to move from unclassified (at the start) to classified (later on). The response was: “*Yes, I have seen more than one Statement of Work drafted in a way where the initial "Phases" or "Work Packages" are performed unclassified with future phases conducted in a classified environment. It would be good to see more of that approach.”*

Alternatives to Traditional Solicitations and Contracts

Commercial Solutions Openings (CSO)

The goal of the CSO is to seek innovative solutions from NDCs. The government must first demonstrate that no traditional contractors were located during market research before it can issue a CSO. A CSO is a solicitation method that is also “combined with” market research on NDCs. The CSO solicitation method can be used to seek innovative solutions for both traditional FAR/DFARS-covered acquisitions (primarily under FAR Part 12) and OTAs. Pursuant to EO 14265 *Modernizing Defense Acquisitions And Spurring Innovation In The Defense Industrial Base,* there “is a first preference for commercial solutions and a general preference for Other Transactions Authority […].”[180]

[180] The White House (2025). *Modernizing Defense Acquisitions and Spurring Innovation in the Defense Industrial Base.* Source: https://www.whitehouse.gov/presidential-actions/2025/04/modernizing-defense-acquisitions-and-spurring-innovation-in-the-defense-industrial-base/



The CSO in plain terms is the basic document and the Area of Interest (AOI) is the document that describes what is needed. Multiple AOIs can be issued against a CSO. Once a CSO is issued, AOIs can typically be issued against it for the duration of the CSO's validity, which is determined by the issuing agency. This period can vary depending on the agency's policies and the specific CSO, but it is common for CSOs to remain open for several years or until the agency decides to close or replace them.

The initial CSO AOI and subsequent AOIs are conducted in three phases, sometimes with a combined Phase 2 and 3:

- Phase 1 (Solution Brief): Offerors submit a concise written white paper (solution brief) that outlines their proposed commercial solution, addressing technical feasibility, alignment with the agency’s needs, and general company qualifications. The evaluation is typically on a Go/No basis.
- Phase 2 (Pitch or Demonstration): Selected offerors from Phase 1 are invited to present their solution in greater detail through an oral presentation, demonstration, or “pitch” session.
- Phase 3 (Full Written Proposal): Those advancing beyond the pitch phase are invited to submit a detailed written proposal. This full proposal includes the technical solution and pricing.

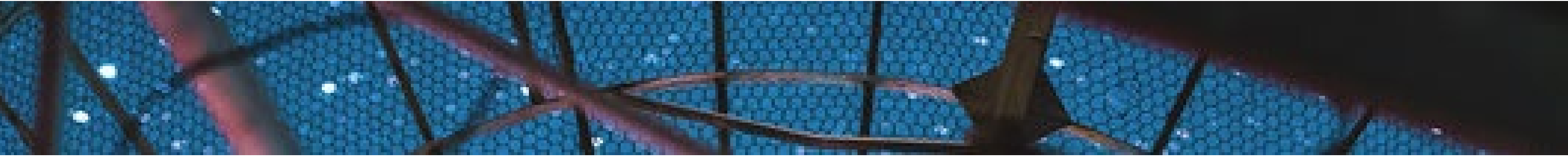
While CSOs must comply with applicable security clearance requirements, it may provide an opportunity to request a DD-254 during the first or second phase. This is key because even if a company submitted a white paper in Phase 1 and was not selected for Phase 2, the company can still participate in future AOIs under that CSO.

Additionally, if the government finds that a Phase 1 white paper under a previous AOI (for which the company was not selected) might apply to a new/different AOI, the government is permitted to invite that company to participate in Phase 2 of the new AOI (without having to participate in that AOIs Phase 1). The window in which the government is permitted to do this is 180 days from that previous Phase 1 submission. Based on the longevity of the CSO and the potential to leverage previous white papers, it seems the Contracting Office would be amenable to completing DD-254s during the first and second phase of the first AOI white paper submission. Therefore, the program office should closely collaborate with the KO to determine if and how the FAST Study’s proposed DD-254 processing approach[181] is practicable for CSOs. (i.e., requiring offerors to submit ECL DD-254 information with their proposals).

Other Transaction Authority (OTAs)

Whether a traditional FAR/DFARS contract or Other Transaction Authority (OTA), *security laws and policies still apply*, as do requirements for the DD-254 and clearances to handle classified documents. It is critical to have clear OTA guides to help the requiring and contracting offices

[181] See *Lack of Entity Clearance Eligibility Sponsorships Creates Barriers to Entry.*



understand what security requirement must be placed in their OTAs based on security laws, codes and policy, and the products or services being procured.

OT Guide Myth 9: ***"None of the federal statutes or regulations apply to OTs."***

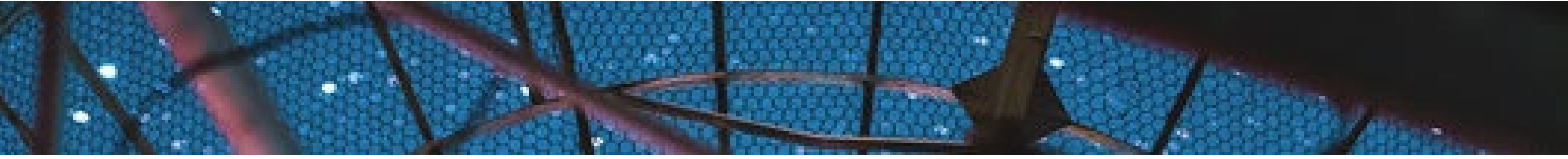
"FALSE. *OT authorities are authorized by law with clear statutory guidelines*. Generally, the statutes and regulations applicable to acquisition and assistance do not apply to OTs. Since OTs are defined in the negative—they are NOT procurement contracts, grants, or cooperative agreements—any statute, regulation, or policy that applies solely to those types of contractual arrangements will not apply to OTs. However, statutes and regulations applicable to acquisition and assistance are only a subset of all federal statutes or regulations. *Laws and regulations that are unrelated to the acquisition or assistance process will still apply to OTs. These can include, but are not limited to*, appropriations, *security, export control, socio-economic, and criminal laws.*"[182]

Given the DATS direction to maximize the use of OTAs, it is reasonable to expect their use to become more common. As such, it is critical to have clear, user friendly, OTA guides to help the requiring and contracting offices understand what security requirements must be placed in their OTAs based on security laws, codes and policy, and the products or services being procured. Exemplar clauses and plain-English tables and matrixes in or accompanying the guide are recommended. Cross-functional teams comprised of acquisition security professionals, physical, personnel and cyber security experts, the KO and a representative(s) from the requiring office should collaborate on discerning what security requirements must and should be included in individual acquisitions as well as new OTA security-specific guides or modifications to the existing OT Guide.

As described in *Integrating Security Throughout the Acquisition Process* section , the OT process and resultant agreements would be better served by enhancing security sections of the OT Guide. For example, "Disclosure and Security, Additional Requirements"[182] lists the following but supplemental guidance and lessons learned should further streamline the OT process to rapidly and securely support the warfighter.

- "To the extent that the OT involves classified information, the Government team shall ensure that the OT agreement is conducted as required by the National Industrial Security Policy outlined in Part 117 of Title 32, Code of Federal Regulations (formerly DOD 5220.22-M) and DD Form 441."
- "To the extent that the OT involves DoD controlled unclassified information, the Government team shall ensure that the OT agreement is conducted as required by DODI 5200.48, Controlled Unclassified Information. Additionally, the Government team should ensure compliance with National Institute of Standards and Technology (NIST) SP 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, for safeguarding the performer's unclassified internal information system."

[182] OUSD(A&S) (2023). *Other Transactions Guide July 2023.* Source: https://www.acq.osd.mil/asda/dpc/cp/policy/docs/guidebook/DoD%20OT%20Guide_July%202023.pdf



- “Compliance with certain statutory prohibitions is also required. These include Section 889 of the FY19 NDAA, Section 1634 of Division A of the NDAA Act for Fiscal Year 2018 (Pub. L. 115-91), and Section 102 of Division R of the Consolidated Appropriations Act, 2023 (Pub. L. 117328)…”
- “To the extent that the OT will involve national security systems, as that term is defined at 44 USC 3252(b) (see 10 U.S.C. 3252), the Government team shall ensure the work under agreement is conducted, as required, to allow for the ability to exclude suppliers on the National Security System Restricted List in SPRS.”
- “The requirements for properly handling and disseminating controlled and restricted information shall flow down to respective personnel, consortium management firms/member, entities, agents, prime/subcontractors, at all levels receiving access to such data. Consulting your Security specialist to ensure the appropriate security requirements and flow down of requirements is a best practice for ensuring proper handling of controlled and restricted data.”

Cooperative Research and Development Agreement (CRADA) – Research and Development

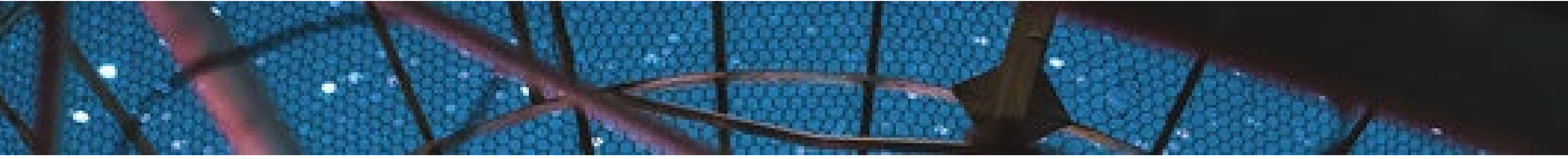
CRADAs are agreements versus contracts. They are authorized under the Federal Technology Transfer Act of 1986 (15 U.S.C. § 3710a), not the FAR. They are specifically designed for research and development collaboration between Federal Laboratories and non-federal entities (e.g., private companies, universities, or other organizations) to advance technology and innovation.

Federal agencies typically do not provide direct funding to the non-federal partner under a CRADA. Instead, they contribute resources like personnel, facilities, or equipment, while the non-federal partner may provide funding or other resources. The resultant rights would need to be negotiated into the agreement. Before entering into the agreement, it is very important to have a vision of what would come next. That is, what does the government intend to accomplish through the CRADA, how will it be applied/used, and what if any agreements or contracts does the government anticipate might follow. The long-term goal should shape what types of rights the government should negotiate into the CRADA so that it can attain its long-term goals which may include a subsequent acquisition resulting in a contract. The non-government entity is typically allowed to commercialize the IP, file for patents, and license it to others, subject to the government’s retained rights.

For classified or sensitive research and development, the government may impose additional restrictions on the use or disclosure of the results. Such restrictions may affect whether the non-government entity wants to enter into a CRADA.

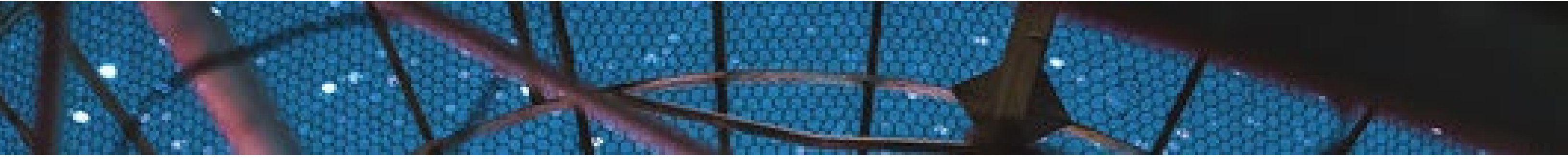
Impact for Warfighter

Implementing the approaches and recommendations discussed in this *Integration of Security into Acquisition Processes and Contracts* section would instill a collaborative, cohesive, informed, and security-focused acquisition process, safeguarding the Warfighter and the essential services and products needed to carry out their mission without compromising the DOW’s ability to balance risks, the prevention or mitigation of security breaches, system downtime, or counter evolving threats.



These actions would enhance DOW's ability to foster innovation that benefits the Warfighter and keeps paces with (or outpaces) advisories' innovation and technology. By embedding acquisition security professionals, security awareness and integration throughout the acquisition lifecycle, streamlining acquisition under FAR Part 12, removing barriers to innovation and entry into the DIB, aligning with DATS, and informing the planning and implementation of DATS, the DOW will be well positioned to "deliver relevant and effective solutions at scale to address warfighting needs" (page 1). Specifically, the actions described would enable the DOW to:

- Foster collaboration among acquisition, security, and program organizations to improve trust, transparency, and communication, accelerating the delivery of secure, mission-ready solutions.
- Develop a skilled and collaborative acquisition workforce to address security challenges, streamline processes, and ensure timely delivery of secure capabilities.
- Increase security awareness throughout the acquisition lifecycle to balance acquisition speed with risk mitigation, preventing security breaches and ensuring operational continuity.
- Integrate security throughout the acquisition lifecycle to deliver reliable, secure, and innovative systems that enhance Warfighter confidence and maintain technological superiority.
- Streamline acquisition under FAR Part 12 to reduce barriers for small businesses and NDCs, fostering innovation and expanding access to the DIB.



4. CONCLUSION

The MITRE FAST Study demonstrates that acquisition security can be tuned to accelerate delivery. Security can be a force multiplier particularly for integrity and resilience, ensuring that cost-effective, competitive, and rapid solutions are delivered to the warfighter uncompromised.

Through rigorous data collection and analyses, MITRE identified 74 challenges including 63 security-focused and 11 acquisition-focused. The most persistent challenges raised across industry concerning entity eligibility, FOCI, and safeguarding of classified and sensitive information were rarely gaps in law or policy. Instead, the challenges stem from inconsistent implementation, fragmented governance, complexities for NDCs, and government non-compliance with security processes. The warfighter experiences these persistent issues not as "compliance friction," but as delayed data, deferred capability, and lost tempo in contested environments. The few policy ambiguities documented by the FAST Study are primarily in cybersecurity. Many NISPOM-specific DOW policies for cybersecurity were built for an earlier era of technology and urgently need updating. For each of the 74 challenges, the FAST Study has identified 155 practical recommended government actions to clarify, automate, modify, and streamline how the Department applies existing security requirements to accelerate mission delivery.

Several themes cut across the challenges and recommended government actions. First, speed to clearance and contract start must improve end-to-end. Unnecessary time lost in entity eligibility, FOCI determination, CPT and CTI identification, PPPs and SCGs, SCIF accreditation, and classified system and network provisioning have direct, cumulative impacts on warfighters. Second, reciprocity and policy harmonization must be real, not aspirational, so the DIB is not forced to debate about identical architectures, markings, or facility determinations in different MILDEPs or regions. Third, data protection needs to be managed as a lifecycle from CPI and CTI, through SCG and PPP, and SSE with interoperable metadata, tagging, and automated marking, not as sets of disconnected instructions. Fourth, oversight of cloud and Zero Trust must align to contractor reality, emphasizing identity and data layer enforcement, standardized cloud evidence packages, and baselines that managed service providers and small businesses can implement. Fifth, automation and AI should be used as force multipliers by digitizing clearance workflows and status tracking, automating form error checking, and ensuring consistent metadata and marking, and integrating threat telemetry under clear governance. Sixth, funding and execution of an independent FOCI Study that is industry data-driven like the FAST Study. Finally, the Department can lower the barriers to entry for small businesses and NDCs by collaborating on the pilot and completion of TurboFCL initiatives and curating a usable plain-English security guidance knowledge hub with repeatable examples and playbooks.

There are near-term actions the DOW must take now at low cost that will have outsized impacts. These include directing DD-254s to be prepared and released by government at solicitation, designating ISSMs as required KMPs for entities clearance eligibility, establishing a mandatory Program Protection Baseline and single CUI Marking and Dissemination Profile across MILDEPs, and rapidly streamlining SF-328/FOCI review and mitigation agreement approval for cleared companies. Longer term, the Department should modernize its security infrastructure and governance by ensuring true personnel clearance reciprocity and enterprise-level classified facilities reciprocity; standing up an integrated cybersecurity enterprise baseline for Zero Trust, cloud; and modernizing the FOCI framework and NDAA Section 847 implementation through a comprehensive, data-driven study.

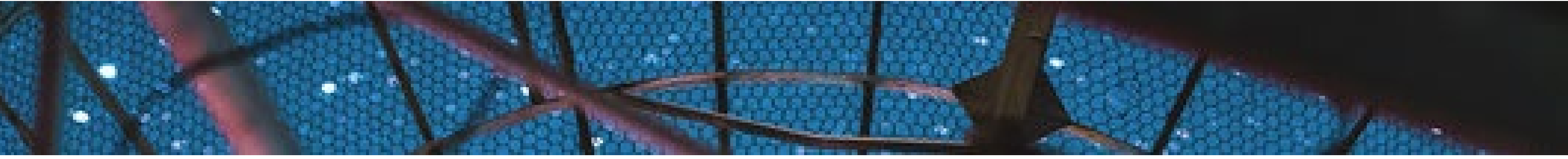
In parallel, DCSA can accelerate DIB innovation reaching the warfighter by shifting from a “gatekeeper” mindset to a customer, service, mission-oriented posture and climate; accelerating SF-328/FOCI triage and mitigation agreements; piloting trusted-company self-certification for additional cleared facilities; and ensuring more consistency and industry-centric focus in operations. Outside the DOW, the Department should work with partners such as DIA, NARA/ISOO, ODNI, and GSA to harmonize SCIF accreditation, CUI and metadata policy, and classified cloud/CIaaS models across the broader national security enterprise.

Progress should be measured the same way programs are judged, by outcomes that matter to the warfighter. The Defense Security Enterprise EXCOM should track and publish reduced median days to entity eligibility and first classified task, higher reciprocity acceptance rates across MILDEPs and regions, lower mismarking and CUI rework rates, faster and more consistent SIPRNet provisioning, and increased participation from small and nontraditional businesses into unclassified then sensitive then classified work. These metrics and status dashboards should be visible to portfolio executives and program offices so leadership can spot bottlenecks, enforce reciprocity, and steer resources where they accelerate delivery.

The FAST Study shows that this is not a call for wholesale policy rewrite. Instead, it is a call to operationalize what already exists, early program protection decisions that are actually made before design, CUI rules that are applied consistently by both government and industry, metadata that can be trusted as the carrier of markings, and cross-domain patterns that are reused rather than reinvented. It is a call to treat SCIFs and classified networks as shared, reusable infrastructure rather than bespoke, one-off projects tied to individual contracts.

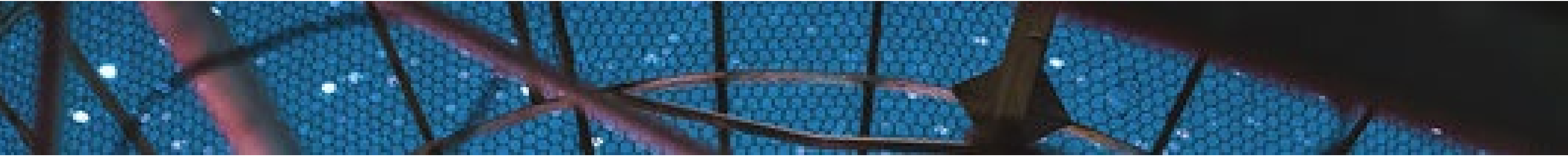
If the Department acts on these recommendations, it will move from reactive security compliance to deliberate security design, from fragmented oversight to unified baselines, from late-stage rework to early, program protection-driven execution. Classified systems and facilities will function as critical mission-enabling infrastructure. Programs will no longer have to design “blind” while they wait for late SCGs and PPPs. Subcontractors, especially small and medium-sized businesses, will be able to participate in classified work without betting the company on unpredictable SCIF access or year-long SIPRNet timelines. Governance conflicts between CIO, I&S, and A&S will be resolved once, centrally, instead of being pushed down to every program and contractor.

The cleared DIB will broaden through practical enablement of small and NDCs. Predictability will return to the acquisition security lifecycle. Faster, more secure delivery, a more resilient industrial base, and better decision dominance for operational forces are within reach. The mission no longer allows a choice between fast and secure. It requires both. The FAST Study offers a clear, actionable path to align both.

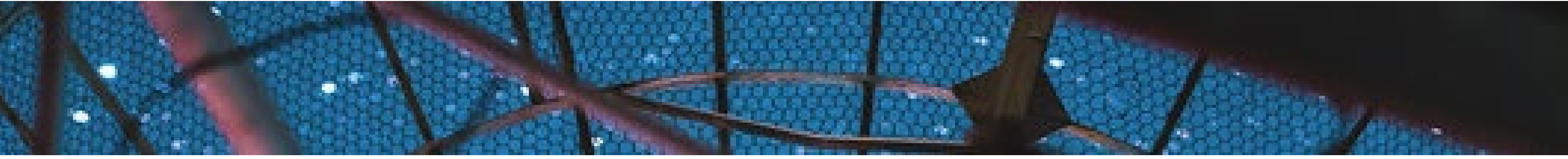


ACRONYMS

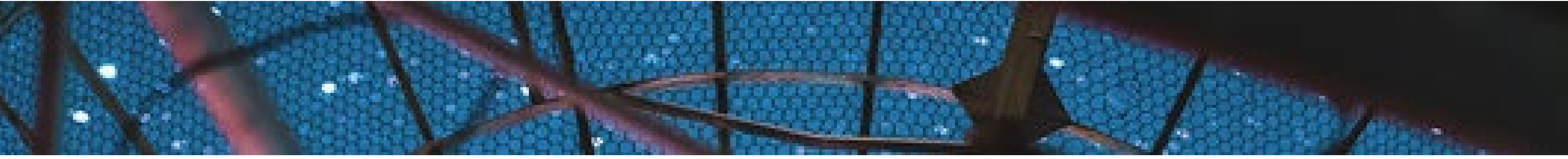
Abbreviation	Full Term
32 CFR 117	Common Federal Rule 32 Section 117 (see NISPOM)
A&A	Assessment and Authorization
AFCEA	Armed Forces Communications and Electronics Association
AOI	Area of Interest
AOP	Affiliated Operations Plan
API	Application Programming Interface
ASCE	Academic Security and Counter Exploitation
ATO	Authority to Operate
BR	Board Resolution
C3PAO	CMMC Third-Party Assessment Organization
CAF	Consolidated Adjudications Facility
CAGE	Commercial and Government Entity Code
CAISSWG	Community Association for Information System Security Working Group
CC SRG	Cloud Computing Security Requirements Guide
CDS	Cross-Domain Solution
CDSE	Center for Development of Security Excellence
CFR	Code of Federal Regulations
CFT	Cross-Functional Teams
CIaaS	Classified Infrastructure-as-a-Service
CIO	Chief Information Officer
CISA	Cybersecurity and Infrastructure Security Agency
CJCSI	Chairman of Joint Chiefs of Staff Instruction
CMMC	Cybersecurity Maturity Model Certification
CMMC 2.0	Cybersecurity Maturity Model Certification, Version 2.0
CNSSI	Committee on National Security Systems Instruction
CoCO	Contracting Officer in Chief
COR	Contracting Officer Representative
CORA	Cyber Operational Readiness Assessment
COTR	Contracting Officer's Technical Representative
CPARS	Contractor Performance Assessment Reporting System
CPI	Critical Program Information
CSMP	Controlled Security Metadata Profile
CSO	Commercial Solution Openings
CSP	Cloud Service Provider
CSSO	Corporate Special Security Officer
CTA	Critical Technology Areas
CTI	Controlled Technical Information
CUI	Controlled Unclassified Information
CV	Continuous Vetting
DAAG	DCSA Assessment and Authorization Guide



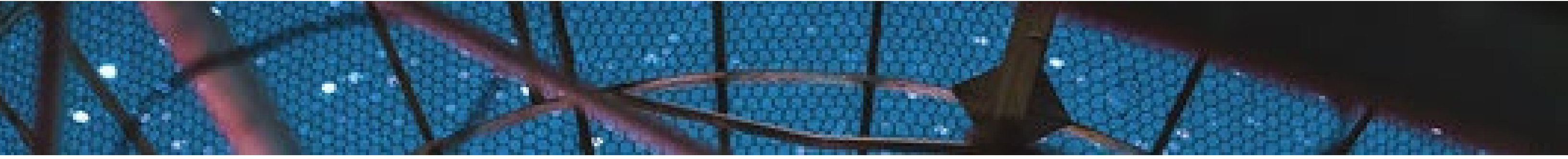
DAAPM	DCSA Assessment and Authorization Process Manual
DARS	DISA Acquisition Regulation Supplement
DATS	Defense Acquisition Transformation Strategy
DAU	Defense Acquisition University
DCMA	Defense Contract Management Agency
DCSA	Defense Counterintelligence and Security Agency
DD-254	Department of Defense Form 254: Contract Security Classification Specification
DESP	DOD Enhanced Security Program (DODI 5205.85)
DFARS	Defense Federal Acquisition Regulation Supplement
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DIB	Defense Industrial Base
DIBCAC	DIB Cybersecurity Assessment Center
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DISN CPG	Defense Information Systems Network Connection Process Guide
DIU	Defense Innovation Unit
DLP	Data Loss Prevention
DOE	Department of Energy
DOW	Department of War
DODAAC	Department of Defense Activity Address Code
DODD	Department of Defense Directive
DODI	Department of Defense Instruction
DODM	Department of Defense Manual
e-APP	Electronic Application
ECL	Entity Clearance
ECMP	Electronic Communications Monitoring Policy
ECP	Electronic Communications Plan
EDR	Endpoint Detection and Response
EO	Executive Order
eSRS	Electronic Subcontracting Reporting System
FAR	Federal Acquisition Regulation
FASC	Federal Acquisition Security Council
FAST	Fast-Tracking Acquisition Security Transformation
FBI	Federal Bureau of Investigation
FCL	Facility Clearance
FedRAMP	Federal Risk and Authorization Management Program
FOCI	Foreign Ownership, Control, and Influence
FOUO	For Official Use Only
FSO	Facility Security Officer
GAO	Government Accountability Office
GBSD	Ground-Based Strategic Deterrent
GCA	Government Contracting Agency



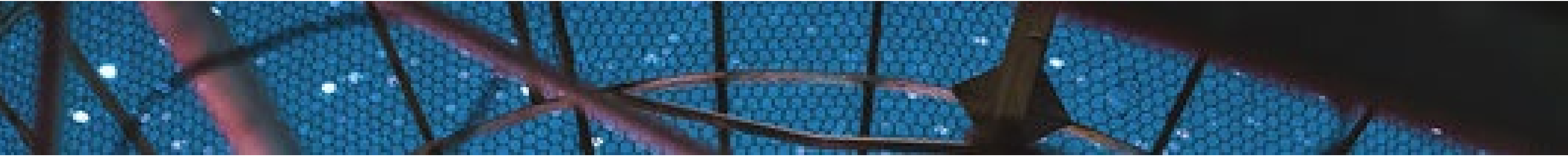
GSA	General Services Administration
GSC	Government Security Committee
IC	Intelligence Community
ICAM	Identity, Credential, and Access Management
ICD	Intelligence Community Directive
ICS	Industrial Control Systems
INSA	Intelligence and National Security Alliance
IPT	Integrated Project Team
ISL	Industrial Security Letter
ISOO	Information Security Oversight Office
ISR	Industrial Security Representative
ISSM	Information System Security Manager
ISSO	Information System Security Officer
ISWG	Industrial Security Working Group
IT	Information Technology
ITPSO	Insider Threat Program Senior Official
JSIG	Joint Special Access Program Implementation Guide
JWICS	Joint Worldwide Intelligence Communications System
KMP	Key Management Personnel
KO	Contracting Officer
MDOC	Mission Defense Operations Center
MILDEP	Military Department
MOS	Military Occupational Specialty
MSP	Managed Service Provider
MTTR	Mean Time To Detect and Recover
NAICS	North American Industry Classification System
NARA	National Archives and Records Administration
NDAA	National Defense Authorization Act
NDC	Nontraditional Defense Contractors
NDIA	National Defense Industrial Association
NI2	NISS Increment II
NIPR	Non-classified Internet Protocol Router Network
NISP	National Industrial Security Program
NISPOM	National Industrial Security Program Operating Manual (see 32 CFR 117)
NISPPAC	National Industrial Security Program Policy Advisory Committee
NISS	National Industrial Security System
NIST	National Institute of Standards and Technology
NIST SP	NIST Special Publication
OD	Outside Director
ODNI	Office of the Director of National Intelligence
OIG	Office of Inspector General
OPM	Office of Personnel Management
OSBP	Office of Small Business Programs



OT	Operational Technology
OTA	Other Transaction Authority
OUSW(A&S), A&S	Office of the Under Secretary of War for Acquisition and Sustainment
OUSW(I&S), I&S	Office of the Under Secretary of War for Intelligence and Security
OUSW(R&E), R&E	Office of the Under Secretary of War for Research & Engineering
PAC PMO	Performance Accountability Council Program Management Office
PAE	Procurement Acquisition Executive
PCL	Personnel Clearance
PEO	Program Executive Officer
PfMO	Portfolio Management Office
PH	Proxy Holder
PKI	Public Key Infrastructure
PM	Program Manager
PMO	Program Management Office
POA&M	Plan of Action and Milestones
PPB	Program Protection Baseline
PPP	Program Protection Plan
PSA	Principal Staff Assistant
PVQ	Personnel Vetting Questionnaire
PWS	Performance Work Statement
R&E	Research & Engineering
RACI	Responsible / Accountable / Consulted / Informed
RD	Restricted Data
RFI	Request for Information
RFP	Request for Proposal
RMF	Risk Management Framework
SaaS	Software-as-a-Service
SAP	Special Access Program
SAPCO	Special Access Program Central Office
SAPF	Special Access Program Facility
SBIR/STTR	Small Business Innovation Research / Small Business Technology Transfer
SBR	Special Board Resolution
SCADA	Supervisory Control and Data Acquisition
SCG	Security Classification Guide
SCIF	Sensitive Compartmented Information Facility
SCRM	Supply Chain Risk Management
SecEA	Security Executive Agent (i.e., ODNI currently)
SETA	Systems Engineering and Technical Assistance
SF-328	Standard Form 328: Certification Pertaining to Foreign Interests
SIPR / SIPRNet	Secret Internet Protocol Router Network
SLA	Service Level Agreement
SMB	Small - and Medium-Sized Businesses
SME	Subject-Matter-Expert

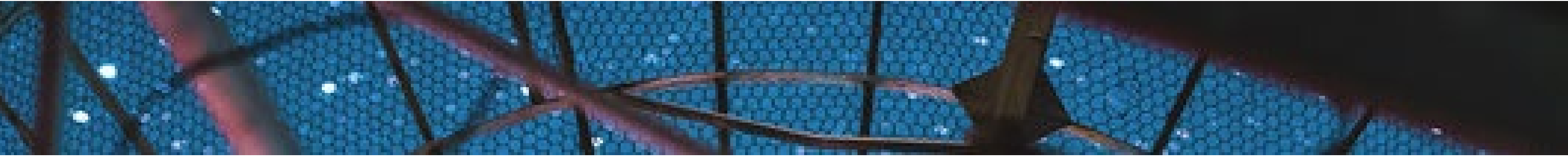


SPF	Sender Policy Framework
SPRS	Supplier Performance Risk System
SSE	System Security Engineering
SSO	Special Security Officer
SSP	System Security Plan
STIX	Structured Threat Information Expression
TAXII	Trusted Automated Exchange of Intelligence Information
TCP	Technology Control Plan
TS//SCI	Top Secret / Sensitive Compartmented Information
TSBOM	Trustworthy Software Bill of Materials
TW 2.0	Trusted Workforce 2.0
UCDSMO	Unified Cross-Domain Services Management Office
UFC	Unified Facilities Criteria
US (if needed)	United States (appears only in references)
USCYBERCOM	United States Cyber Command
VC	Venture Capital
ZT	Zero Trust
ZT PfMO	Zero Trust Portfolio Management Office



APPENDIX A: INTERVIEW TOPICS

1. **Most Challenging Security Requirements, Practices, and Systems**
   a. Burdensome requirements, practices, and systems which impede award, start, and delivery
   b. Requirements, practices, and systems that decrease quality or increase cost
   c. Misunderstood or misapplied requirements, practices, and systems (and consequences)
   d. Compliance-only requirements, practices, and systems
   e. Essential-to-keep requirements, practices, and systems
   f. Changes in the threat landscape not reflected in current requirements, practices, and systems
2. **Entity Clearance Eligibility and Access**
   a. Sponsorship dynamics, including prime contractor versus government sponsorship
   b. Maintaining Entity Clearance Eligibility between classified projects and the role of need-to-know
3. **FOCI**
   a. Burdens within the FOCI review and mitigation process
   b. Earlier assessment and mitigation for unclassified work and for non-NISP companies
   c. Practical improvements to timelines and clarity
   d. NDAA Section 847 implementation
4. **Safeguarding Sensitive and Classified Information**
   a. Handling, transmitting, and storing CUI and classified information
   b. Requirements to cancel, retain, or modernize
   c. Earlier protection options for sensitive information prior to classification
5. **PPPs, SCGs and DD Form 254**
   a. Usability and timeliness of PPPs, SCGs, and DD-254s from government and from prime contractor
   b. Flowdown challenges to subcontractors and recommended improvements
6. **Classified Facilities**
   a. Collateral, SCIF, and SAPF accreditation, audit, and reaccreditation challenges
   b. Reciprocity and co-use barriers across programs and agencies
   c. Experience with third-party auditors, self-assessment, and approval delegation
   d. Reciprocal use of classified facilities across MILDEPs/programs
7. **Classified Information Networks and Systems (e.g., SIPRNet, JWICS)**
   a. Access and accreditation for classified networks
   b. Initial authorization, audit, reaccreditation, and maintenance challenges
   c. Opportunities to streamline and standardize policy interpretations
   d. Reciprocal use of secure information networks and systems across MILDEPs/programs
8. **Cybersecurity and Information Security Requirements, Practices, and Systems**
   a. Burdens associated with overlapping frameworks and controls
   b. Impacts on award and delivery timelines
   c. Modernization needs for small businesses, medium-sized businesses, and NDC
9. **Security Aspects of Subcontracting**
   a. Prime contractor's subcontractor compliance management and support practices
   b. Subcontractor access to guidance, sponsorship, and security flowdowns
   c. Government roles that would improve security of subcontractor pathways
10. **Security Cost and Financing**
    a. Reimbursable security costs vs. costs that should remain contractor's responsibility
11. **Security Challenges in Business Development**
    a. Programs/approaches enabling industry organizations to enter classified work
    b. Use of Other Transaction Agreements (OTAs) and their security implications
    c. Role of Security Integrators in helping organization meet government security requirements and enter classified work markets
    d. Finding classified work and improving government support channel



APPENDIX B: ENTITY CLEARANCE CHALLENGES AND SOLUTIONS FOR NI2 IMPLEMENTATION

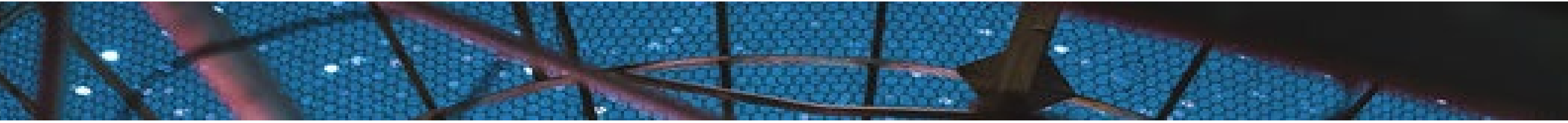
Table 9. Entity Clearance Challenge Descriptions

Challenge	Description
Industry lacks transparency on Entity Clearance status	• Lack of real-time, graphical visibility into Entity Clearance status • Current opacity hinders budgeting and staffing for DOW contracts • Many contractors cannot begin work until Entity Clearance approval, delaying project starts • Other contractors are limited to Secret-level tasks while awaiting TS//SCI approvals, slowing delivery • Friction deters NDCs and erodes trust in government processes
Current Entity Clearance package submission process involves outdated email exchanges, spreadsheet tracking, and lack of consistent automated error checking	• Reliance on manual exchanges of Entity Clearance documents (e.g., via e-mail) create inefficiency and single point of failure • Lack of shared, real-time status tracking creates bottlenecks for DCSA and industry as action owners are not clearly delineated • Stop-and-return workflow returns packages after first error instead of iteratively resolving issues, slowing progress • Lack of consistent automated upfront validation leaves errors unresolved until later in the process, increasing delays and rework • Absence of ticketing system slows momentum, prioritization of urgent items, and coordination of parallel actions
DCSA receiving high levels of erroneous Entity Clearance package submissions	• ~50% of initial Entity Clearance submission packages returned due to errors, increasing delays, rework, and straining DCSA resources • DCSA does not provide API for industry solutions (e.g., TurboFCL[183]) to submit data directly to DCSA, forcing more time-consuming and error-prone manual transfers (e.g., e-mail) • Lack of consistent automated upfront validation leaves errors unresolved until later in the process, increasing delays and rework

DCSA should take the following actions:

- Implement real-time whole-of-Entity Clearance graphical status tracker module, delivering process tracking and visibility feature repeatedly requested by industry interviewees.
- Integrate Entity Clearance graphical status tracker with ticketing system to provide shared, real-time visibility for DCSA and industry. Integration should display status, action owners, and bottlenecks, eliminating the need for back-and-forth emails and frequent industry calls to DCSA's helpline. It will also enable issues to be addressed in parallel, reducing delays caused by repeated resubmissions.
- Implement automated error checking capabilities at package submission to quickly assess for errors and submit to ticketing system for resolution by industry.
- Develop a standard API for DCSA to receive outputs from solutions (e.g., TurboFCL), to expedite the Entity Clearance process by decreasing errors and reducing manual data transfer effort**.**
- Enable industry to make multiple, concurrent change conditions.

[183] See *Complexity and Challenges in Industry Entity Clearance Eligibility Preparation*



APPENDIX C: SUBCONTRACTOR FLOWDOWNS TABLE

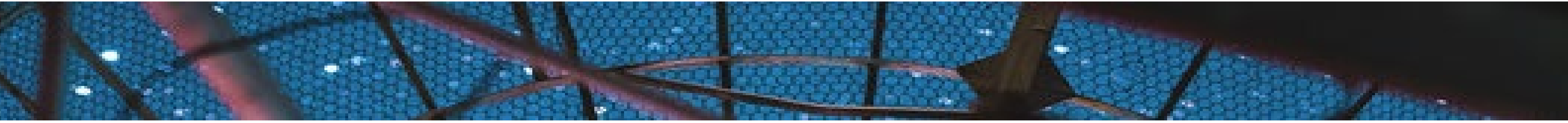
The tables in this Appendix summarize security-related clauses, including subcontractor flowdown requirements, with links to FAR and DFARS. They highlight key points rather than full clause details. Complete text and prescriptions are accessible via the hyperlink. The inclusion of FAR and DFARS clauses in a prime contract is determined by the Contracting Officer based on prescriptions and policy. These tables serve as a reference, not an exhaustive or authoritative source. FAR and DFARS are subject to change due to the FAR overhaul. The FAR overhaul impacts on DOW have not yet been determined/confirmed. After the FAR determinations/confirmations, DFARS updates would be made accordingly. The FAR Overhaul Impact column in the below table describes *potential* impacts.

Unless otherwise noted, the below would apply to solicitations and contracts. FAR and DFARS clauses are used for acquisitions conducted under the FAR and DFARS. If an acquisition is conducted under the Other Transaction Authority (OTA), the program, security and contracting offices must work together to ensure security is addressed as required by law, statute and policy pertaining to security. Using an OTA does not exempt the government from complying with security.

Table 10. Information, Classified and Disclosure

Clause	Brief Description	Applies To	FAR or DFARS Prescriptions	Flowdown Required?	Of Note	Potential FAR Overhaul Impact
FAR 52.204-2 Security Requirements **FAC#**2025-06 Effective 10/01/25	Protection of classified information (Confidential, Secret, Top Secret)	Access to classified information under the contract	FAR Subpart 4.4 - Safeguarding Classified Information Within Industry **As prescribed in:** FAR 4.404. The CO **shall** insert the clause in solicitations and contracts when the contract may **require access** to classified information [as	(d) The Contractor agrees to insert terms that **conform substantially** to the language of this clause, **including this paragraph (d)** but excluding any reference to the Changes clause of this contract, in all subcontracts under this contract that involve access to classified information.	(c) If, subsequent to the date of this contract, the security classification or security requirements under this contract are changed by the Government and **if the changes cause an increase or decrease in security costs or otherwise affect any other term or condition of this contract, the contract shall be subject to an equitable adjustment** as if the changes were directed under the Changes clause of this contract. *[The clause prescribes Alternate Text*	Security requirements consolidated, no material changes to classified information clause; Part 4 streamlining[184]

[184] Wiley Rein LLP. *Decoding the FAR Overhaul (2025)*. Source: https://www.wiley.law/decoding-the-far-overhaul



			DOW is covered by NISP]		*for R&D, Educational Institutions and Construction]*	
DFARS 252.204-7000 Disclosure of Information DFARS Change#: 10/24/2025 Effective Date: 10/24/2025	Restricts release of unclassified info; requires DOW approval	Contracts with sensitive DOW information	**As prescribed in**: DFARS 204.404-70(a)	(c) The Contractor agrees to include a **similar requirement, including this paragraph (c)**, in each subcontract under this contract. [See "Of Note" for remainder of clause.]	The clause states [s]ubcontractors shall submit requests for authorization to release through the prime contractor to the Contracting Officer	Overhaul strengthens approval triggers and recordkeeping[184]

Unless otherwise noted, the below would apply to solicitations and contracts. FAR and DFARS clauses are used for acquisitions conducted under the FAR and DFARS. If an acquisition is conducted under the Other Transaction Authority (OTA), the program, security and contracting offices must work together to ensure security is addressed as required by law, statute and policy pertaining to security. Using an OTA does not exempt the government from complying with security.

Table 11. Cybersecurity

Clause	Brief Description	Applies To	FAR or DFARS Prescriptions	Flowdown Required?	Of Note	Potential FAR Overhaul Impact
FAR 52.204-21 Basic Safeguard-ing of Covered Contractor Information Systems	Safeguard-ing covered contractor info systems (Federal Contract Information)	All except COTS contracts	**As prescribed in:** FAR 4.1903:	c) *Subcontracts.* The Contractor shall **include the substance of this clause, including this paragraph (c),** in subcontracts under this contract (including subcontracts for the acquisition of commercial products or commercial services, **other than commercially available off-the-shelf items**), in which the subcontractor may have Federal contract information residing in or transiting through its information system.		Incident reporting strengthened, basic safeguarding retained, CMMC alignment[185]

[185] Federal Register (2025). *Federal Acquisition Regulation: Controlled Unclassified Information.* Source: https://www.federalregister.gov/documents/2025/01/15/2024-30437/federal-acquisition-regulation-controlled-unclassified-information

DFARS 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting Change Number: 10/24/2025 Effective Date: 10/24/2025	Safeguard-ing Covered Defense Info, NIST SP 800-171 controls	DOW contracts process-ing Covered Defense Info.	**As prescribed in:** DFARS 204.7304 (c)	The Contractor shall- (1) Include this clause, including this paragraph (m), in subcontracts, or similar contractual instruments, for operationally critical support, or for which subcontract performance will involve covered defense information, including subcontracts for commercial products or commercial services, without alteration, except to identify the parties. The Contractor shall determine if the information required for subcontractor performance retains its identity as covered defense information and will require protection under this clause, and, if necessary, consult with the Contracting Officer; and **[The "Of Note" column to the right includes the remainder of the paragraph "(m) text.]**	The Contractor shall- (2) Require subcontractors to - (i) Notify the prime Contractor (or next higher-tier subcontractor) when submitting a request to vary from a NIST SP 800-171 security requirement to the Contracting Officer, in accordance with paragraph (b)(2)(ii)(B) of this clause; and (ii) Provide the incident report number, automatically assigned by DOW, to the prime Contractor (or next higher-tier subcontractor) as soon as practicable, when reporting a cyber incident to DOW as required in paragraph (c) of this clause.	CMMC phased implementation and SP 800-171 requirements under overhaul[186]
DFARS 252.204-7020 NIST SP 800-171DOW Assessment Requirements **Change Number:** DFARS	Government access/audit of NIST SP 800-171 compliance	Applies if DFARS 252.204-7012/7019 are included	**As prescribed in:** DFARS 204.7304(e)	(g) Subcontracts. (1) The Contractor shall **insert the substance of this clause, including this paragraph (g)**, in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial products or commercial services (excluding commercially available off-the-shelf).	(2) The Contractor shall not award a subcontract or other contractual instrument, that is subject to the implementation of NIST SP 800–171 security requirements, in accordance with DFARS clause 252.204–7012 of this contract, unless the subcontractor has	Overhaul aligns enforcement and audit rights with CMMC[186]

[186] Skadden, Arps, Slate, Meagher & Flom LLP and Affiliates (2025). *DOW Finalizes DFARS Cybersecurity Certification Rule: What Contractors Need to Know* https://www.skadden.com/insights/publications/2025/09/dod-finalizes-dfars-cybersecurity-certification-rule

Change 10/24/2025 Effective Date: 10/24/2025				[The "Of Note" column to the right includes the remainder of the paragraph "(g) text.]	completed, within the last 3 years, at least a Basic NIST SP 800–171 DOW Assessment, as described in https://www.acq.osd.mil/asda/dpc/cp/cyber/docs/safeguarding/NIST-SP-800-171-Assessment-Methodology-Version-1.2.1-6.24.2020.pdf , for all covered contractor information systems relevant to its offer that are not part of an information technology service or system operated on behalf of the Government. (3) If a subcontractor does not have summary level scores of a current NIST SP 800-171 DOW Assessment (i.e., not more than 3 years old unless a lesser time is specified in the solicitation) posted in SPRS, the subcontractor may conduct and submit a Basic Assessment, in accordance with the NIST SP 800-171 DOW Assessment Methodology, to mailto:webptsmh@navy.mil for posting to SPRS along with the information required by paragraph (d) of this clause.	

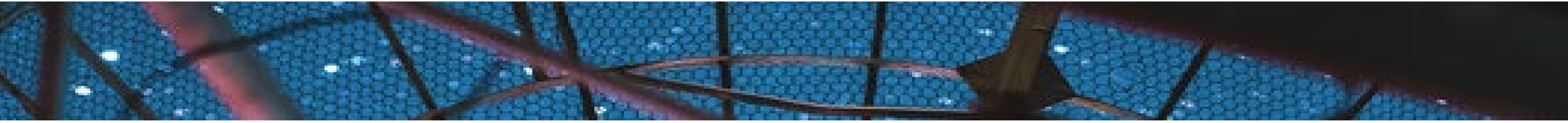


Table 12. Cloud Security

Clause	Brief Description	Applicable	FAR or DFARS Prescriptions	Flowdown Required?	Of Note	Potential FAR Overhaul Impact
DFARS 252.239-7010-Cloud-Computing-Services	Security for cloud services; FedRAMP/FIPS compliance	DOW contracts for cloud services	**As prescribed in**: DFARS 239.7604 (b)	(l) *Subcontracts*. The Contractor shall include this clause, including this paragraph (l), in all subcontracts that involve or may involve cloud services, including subcontracts for commercial services.		To be determined
FAR 52.239-XX (proposed)	Proposed Security controls for federal systems using cloud [187]	Info systems contracts, agency-specified FIPS	As prescribed in: FAR Part 39 (proposed)	Proposed: expected to require flowdown for cloud-based subcontractors https://www.federalregister.gov/documents/2025/01/15/2024-30437/federal-acquisition-regulation-controlled-unclassified-informationfederalregister	Clause is not yet in effect. It is included as a proposed clause.[188]	Pending; alignment with FedRAMP, NIST, agency guidance[189]

[187] Proposed FAR rule for standardizing cybersecurity requirements for federal information systems that use cloud computing services: requires contractors to implement and maintain security controls based on the contract's specified FedRAMP level and to perform continuous monitoring. It also mandates data must be stored within the U.S. for high-impact (as defined by FIPS-199) systems and specifies data handling and disposal requirements.

[188] Proposed FAR rule for standardizing cybersecurity requirements for federal information systems that use cloud computing services: requires contractors to implement and maintain security controls based on the contract's specified FedRAMP level and to perform continuous monitoring. It also mandates data must be stored within the U.S. for high-impact (as defined by FIPS-199) systems and specifies data handling and disposal requirements.

[189] Federal Register (2025). *Federal Acquisition Regulation: Controlled Unclassified Information.* Source: https://www.federalregister.gov/documents/2025/01/15/2024-30437/federal-acquisition-regulation-controlled-unclassified-information

MITRE | National Security Engineering Center

MITRE FAST Study Team:

Dr. Deanna D. Caputo, PL
Dr. James Doodson, TL
Dr. W. Bryan Higgins
Tracy Cassidy
Emily Pitek
Chris Folk
Janet Olcott
Joan Grimson
Sarah Velez