

Office of the Under Secretary of War for Intelligence and Security OUSW(I&S)

Patrick Harris | OUSW(I&S)/CL&S/IAP

Jamie Long | OUSW(I&S)/CL&S/IAP

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

2026 VIRTUAL DCSA SECURITY CONFERENCE

SEPTEMBER 14 - 18, 2026 | PROTECT OUR POTENTIAL



Acquisition and Industrial Security Policy Update Brief



- Acquisition Security
- Overview
- The Fast-Tracking Acquisition Security Transformation (FAST) Study
- Classified-Infrastructure-as-a-Service (ClaaS)
- The Modernization Blueprint: Our Three Pillars for Reform
- From Insight to Action: Key Reforms and Next Steps
- Conclusion & Contact Information

The Acquisition Security Imperative



By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered:

Section 1. Purpose. As Chief Executive and Commander in Chief, I am committed to ensuring that the United States military possesses the most lethal warfighting capabilities in the world. America's defense industrial base is central to this effort. Similarly, the defense acquisition workforce is a national strategic asset that will be decisive in any conflict, where the factory floor can be just as significant as the battlefield.

Unfortunately, after years of misplaced priorities and poor management, our defense acquisition system does not provide the speed and flexibility our Armed Forces need to have decisive advantages in the future. In order to strengthen our military edge, America must deliver state-of-the-art capabilities at speed and scale through a comprehensive overhaul of this system.

Sec. 2. Policy. It is the policy of the United States Government to accelerate defense procurement and revitalize the defense industrial base to restore peace through strength. To achieve this, the United States will rapidly reform our antiquated defense acquisition processes with an emphasis on speed, flexibility, and execution. We will also modernize the duties and composition of the defense acquisition workforce, as well as incentivize and reward risk-taking and innovation from these personnel.

Sec. 3. Acquisition Process Reform. Within 60 days of the date of this order, the Secretary of

“...the United States will rapidly reform our antiquated defense acquisition processes with **an emphasis on speed, flexibility, and execution**. We will also modernize the duties and composition of the defense acquisition workforce, as well as **incentivize and reward risk-taking and innovation** from these personnel.”

Acquisition Security is how DoW leverages contract requirements and modernizes security requirements to achieve acquisition reform objectives

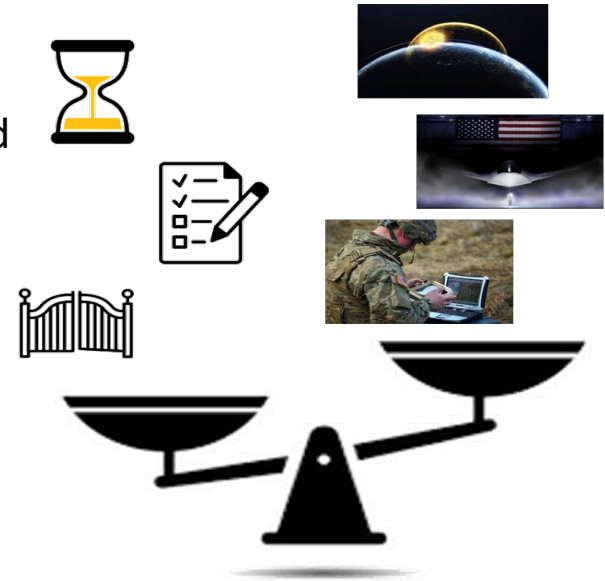
Integration of security requirements and considerations throughout acquisition lifecycles



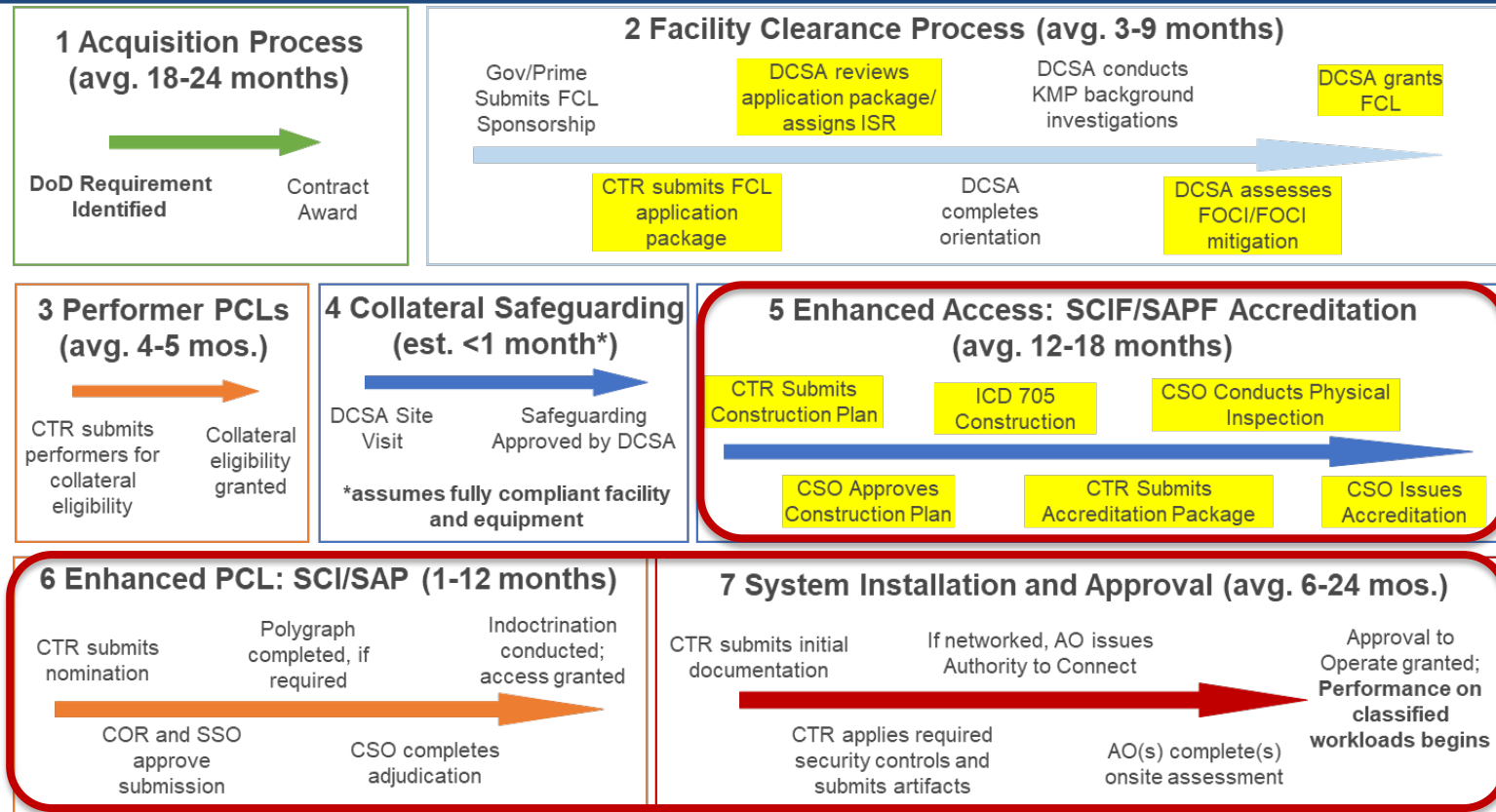
Modernized security administration and oversight capable of the speed and agility required for rapid, and protected, acquisitions

Redefining Risk: How Our 'Security' Culture Endangers the Mission

- Current risk posture **mistakes process compliance for risk reduction** – prioritizing avoidance of near-term, bureaucratic threats over achieving national security outcomes
- This creates a dangerous paradox: the **fear of manageable, short-term process risks leads directly to unacceptable strategic failures** – late delivery of critical capabilities, a stifled and shrinking industrial base (NISP), and the ceding of initiative to our adversaries
- Shifting from **risk aversion to mature risk management** demands a new calculus – explicitly analyzing and accepting smaller, immediate process risks in exchange for the overwhelming mission benefits of speed, innovation, and timely warfighter advantage



Current Classified Performance Security Requirements



Fast-tracking Acquisition Security Transformation (FAST) Study

- OUSW(I&S) sponsored initiative **to identify security processes** where bureaucracy increases risk instead of reducing it
- April 2025 – June 2025: FAST researchers interviewed government leaders from OUSW(I&S), OUSW(R&E), OUSW(A&S), SAPCO, DUSN, HQDA, USAF, DARPA, DIU, DISA, WHS, DCSA, ISSO, and PAC PMO to **baseline process context** and intent and support actionable recommendations to **support effective change**
- July 2025 – December 2025: FAST team conducted focus groups, interviews, and surveys to gather data from over 6,700 representatives from industry to **identify friction points** and develop **data-backed recommended** solutions
- January 2026 – March 2026: Public release and report socialization to engage with stakeholders and gather initial feedback
- April 2026 – June 2026: Finalize POAM and begin quarterly reporting

FAST Study Key Findings

- Core obstacles rooted in execution, not policy: fragmented governance, outdated processes, and a **security culture disconnected** from the speed of mission
- 74 challenge areas with 155 practical recommendations to transform acquisition security **from a reactive compliance function to a proactive enabler** of speed and innovation
- Recommendations are intentionally worded to capture context from volumes of interviews and data; not the only possible solution but alternatives should be carefully crafted to address the correct problem
- Describes a system that is **failing** to **deliver** critical **warfighter capabilities**
- Current processes were built for a paper world **operating in static locations**; incremental change isn't working and hasn't worked for a long time
- The solution is not a concrete overhaul, but an **adaptive mission-focused** stance that ensures the enterprise is postured to **integrate Cloud, AI, Quantum, and emerging capabilities**

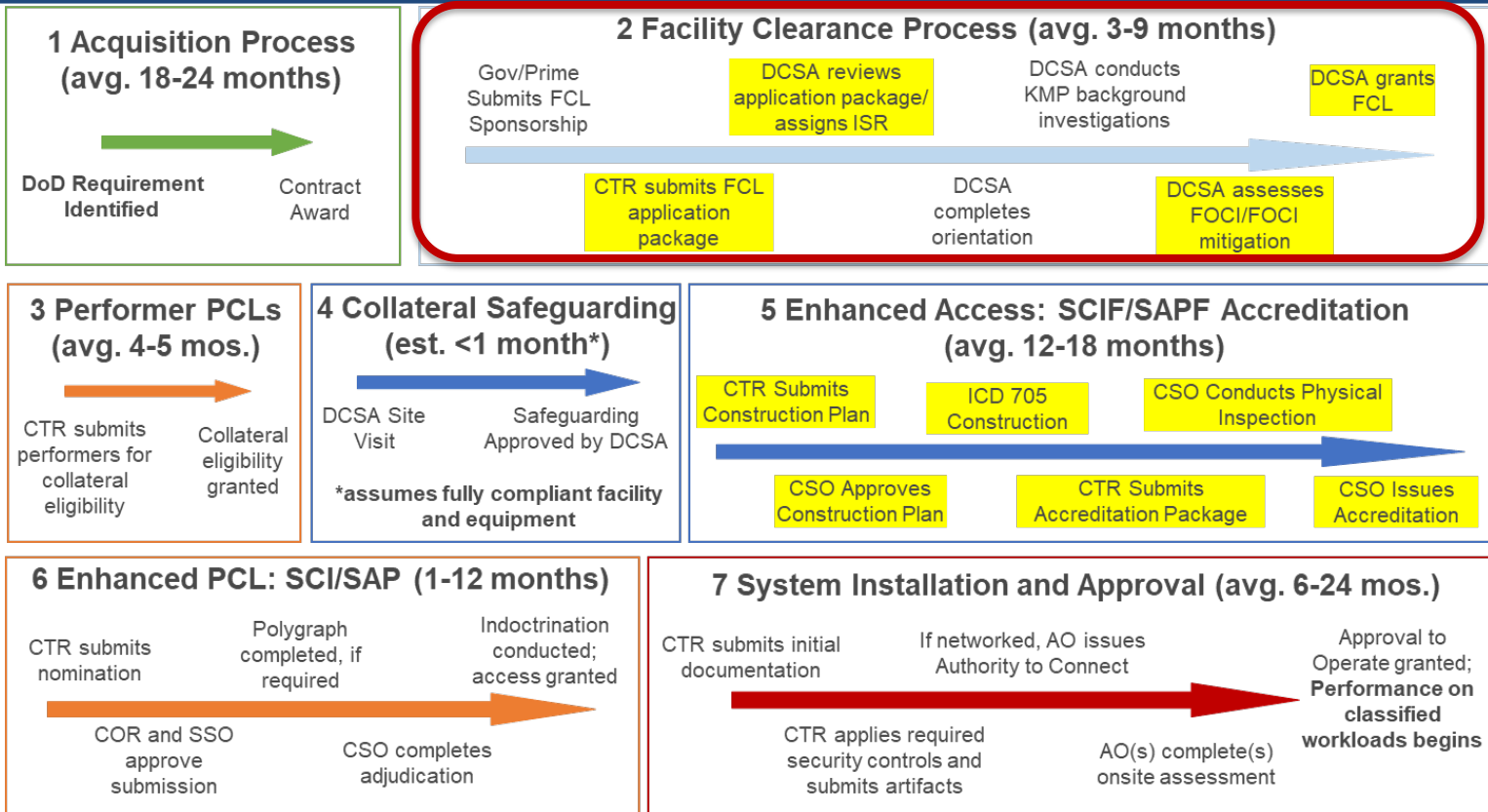


Classified-Infrastructure-as-a-Service (ClaaS)

- Commercial ClaaS offers partial solutions for Entity Access and Safeguarding classified and sensitive information challenge areas
- ClaaS provides a time saving avenue to leverage existing infrastructure
- ClaaS provides a viable infrastructure solution to meet warfighter requirements in full previously underserved regions



Current Classified Performance Security Requirements



Industrial Security: A Framework Out of Time

- **Pre-Digital Design:** Legacy industrial security policies—including DoD Manual 5220.32, Volume 1—were built for a pre-digital, facility-centric era
- **Operational Friction:** This outdated approach is misaligned with modern technology, speed, and threats, slowing down critical capability delivery to the warfighter



The Core Problem: Legacy Model vs. Modern DIB

- **The "1990s" Gap:** We are applying a paper-based, 1993 National Industrial Security Program (NISP) model to a 2020s cloud-based, globally interconnected Defense Industrial Base (DIB)
- **Systemic Strain:** Recent findings from both the GAO Industrial Security Report and the MITRE FAST Study show this mismatch creates structural bottlenecks that stifle innovation and introduce unnecessary risk

Reforming DoWM 5220.32, Vol. 1

- **Data-Driven Modernization:** The GAO and MITRE FAST data provides the Department of War a concrete baseline to modernize acquisition and industrial security oversight
- **Targeting Friction Points:** Direct reforms are targeting legacy barriers in facility clearance (FCL) eligibility, FOCI, safeguarding, and classified access—specifically to ease entry for small and non-traditional defense partners



From Insight to Action: Our Modernization Blueprint

Pillar of Action	Strategic Goal
1. Modernize the Policy	Evolve DoWM 5220.32 from a static rulebook into a dynamic, risk-based framework that enables speed and security.
2. Empower the Field	Arm our security professionals with the tools, training, and authority to make consistent, data-driven decisions.
3. Build a True Partnership	Transform our relationship with the DIB from transactional oversight to collaborative, mission-focused partnership.



Modernizing the Manual: Risk-Based Oversight in Practice

Outdated Mandate	The New Risk-Based Policy
The Problem: The rigid 12/18-month security review cycle in DoDM 5220.32 is unsustainable and treats all facilities as equal risks.	The Solution: We are formally updating the manual to establish a 36-month security review cycle for lower-risk facilities. This is a deliberate policy shift to a risk-based model.
The Impact: It was impossible to meet the old mandate, leading to missed reviews and forcing our workforce to focus on low-value compliance tasks.	The Outcome: This change frees up critical DCSA resources to focus on high-sensitivity facilities and emerging threats. It allows us to manage risk intelligently instead of just managing a calendar.
The Timeline: This policy change is happening now!	



Empowering the Field: Consistent Execution Through Tools & Process

Challenge	Corrective Action & Impact
"Zip-Code Security" & Inconsistent Oversight: The GAO identified that reviewers lacked standardized tools and uniform analytical methods, leading to unpredictable regional risk assessments.	Deliver Standardized Analytic Tools (Dec 2026): DCSA is developing and deploying enterprise analytic tools across all field offices, ensuring consistent, data-driven oversight nationwide.
Operational Silos & Bureaucratic Drag: Fragmented oversight structures created internal friction, slowed review turnaround times, and diluted operational accountability.	Consolidate Operations & Realign Roles: DCSA completed a major reorganization of Industrial Security and Field Operations into a unified command—streamlining reporting and prioritizing high-risk facilities.



Policy Alignment: Transitioning from FCL to EED

The Problem: Legacy Construct	The Solution: Modern Policy Alignment
"Facility Security Clearance (FCL)": Conveys that a physical building, vault, or dedicated SCIF is required before an organization can be vetted or trusted.	"Entity Eligibility Determination (EED)": Clarifies that the organization/legal entity (and its Key Management Personnel) is evaluated for trustworthiness and classified access.
Industry Confusion & Barrier to Entry: As identified in the MITRE FAST Study, non-traditional and small software firms are deterred by the false premise of real estate overhead.	Federal Policy Synchronization: Formally aligns DoWM 5220.32 terminology with 32 CFR Part 2004 (NISP) and 32 CFR Part 117 (NISPOM Rule), separating entity vetting from physical safeguarding.



Structural Policy Reform: Eliminating the "Two-Year Cliff"

The Problem: Legacy Constraint	The Solution: FAST Study Recommendation
The "Two-Year Cliff": Current policy forces the administrative termination of entity and personnel eligibility after a 24-month break in access.	5-Year Eligibility Horizon: Extend the administrative termination window to five years, aligning entity lifecycle rules with continuous vetting standards.
Operational Impact: Drives unnecessary, costly reinvestigations and creates severe friction when re-engaging proven commercial innovators.	Operational Outcome: Reduces administrative churn for DCSA, cuts re-entry costs for industry, and preserves cleared talent and vendor capacity across contract cycles.

Delivering on the Modernization Blueprint

Pillar of Action	Key Transformation
1. Modernize the Policy	• DoWM 5220.32 Reform: 36-month risk-based review cycle. • Entity Over Facility: Adopting EED under 32 CFR Part 2004. • Retain Talent: Eliminating the "two-year cliff" with a 5-year window.
2. Empower the Field	• Standardized Analytics: Deploying field tools by Dec 2026. • Consistent Oversight: Eliminating "zip-code security."
3. Build a True Partnership	• Customer Success: Dedicated office for stakeholder support.



Questions/Comments



Contact Information

Patrick N. Harris

OUSW(I&S)CL&S IAP

Chief, Acquisition Security and Risk Mitigation Division

patrick.n.harris7.civ@mail.mil

Jamie E. Long

OUSW(I&S)CL&S IAP

Chief, Industrial Security Policy & Oversight Division

Jamie.e.long2.civ@mail.mil

