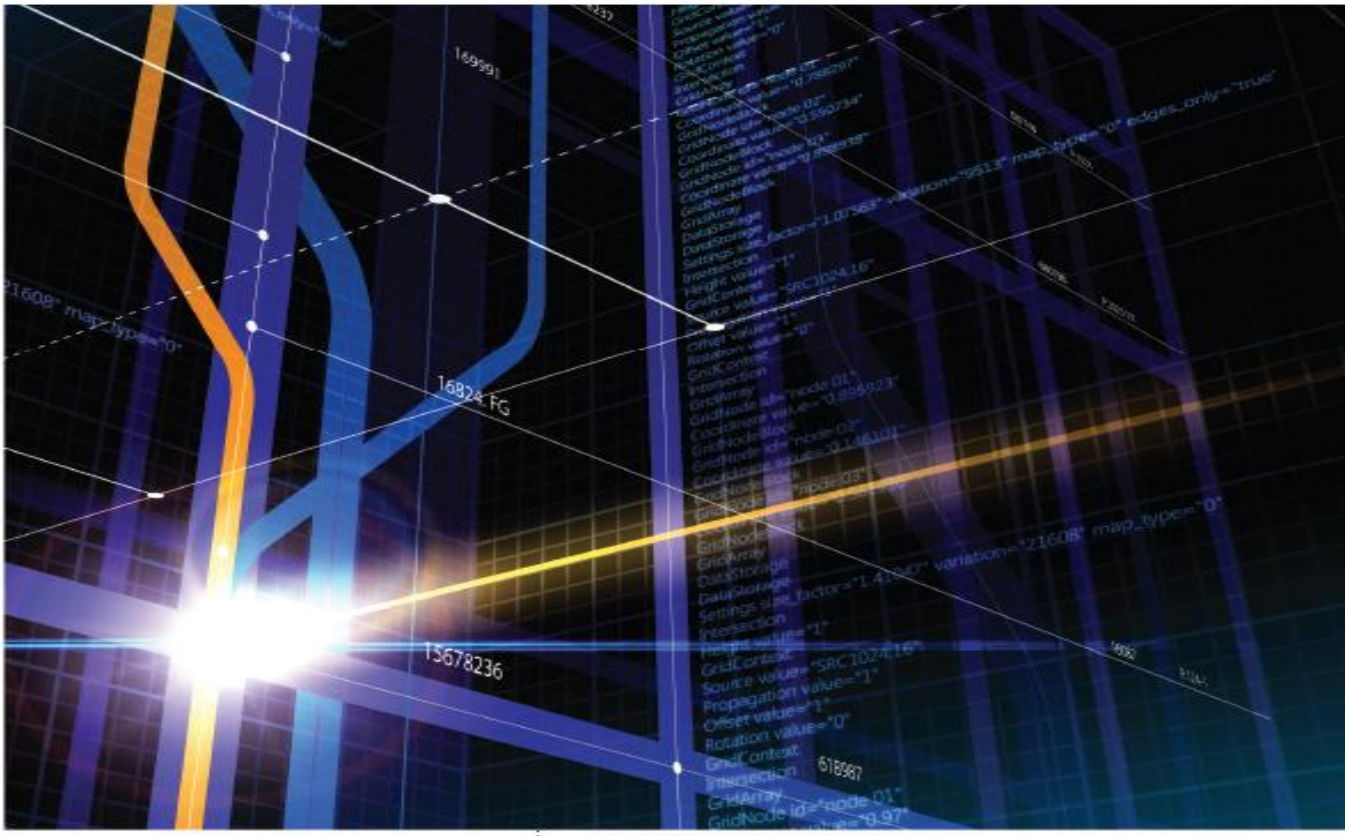
EO 14265 Public Comment Submission

A Roadmap for Sustainable IT Acquisition Reform 2.0

A Digital Transformational Guide for the 47th President and Executive Branch Leadership



IT Acquisition Advisory Council
904 Clifton Drive
Alexandria, Virginia 22308
703.768.0400 703.765.9295 *f*
www.IT-AAC.org

EO 14265 Public Comment Submission

Docket No.: DoD-2025-OS-0018

Title: Executive Order 14265 – Modernizing Defense Acquisitions and Spurring Innovation in the Defense Industrial Base

Submitted by IT-AAC and FDD:

- John Weiler – CEO and CoFounder, Information Technology Acquisition Advisory Council (IT-AAC)
- Georgianna Shea - Foundation for Defense of Democracies (FDD)
- Dick Brooks – Business Cyber Guardian (BCG)
- Daniel Ragsdale – Former Assistant National Cyber Director
- Michele Iverson – Former Director, Risk Assessment & Operational Integration, DOD CIO
- Harry Wingo – Former Deputy National Cyber Director

www.IT-AAC.org www.FDD.org

Date: August 8, 2025

Executive Summary

This comment responds to the Department of Defense's request for public input on Executive Order 14265. We strongly support the EO's mission to accelerate defense procurement, reduce systemic inefficiencies, and expand opportunities for small businesses that deliver innovative technologies. To achieve this, DoD must address persistent cultural, process, and security challenges across the acquisition ecosystem.

Our recommendations are organized across six priority areas critical to implementing EO 14265:

1) **People: Workforce Readiness and Cultural Transformation** – Reform workforce incentives to reward secure innovation and timely delivery. Modernize DAU training, embed real-time threat intelligence, deploy Agile Tiger Teams, and reduce reliance on SETA contractors. Cultivate a mission-driven culture through mentoring and case-based learning.
2) **Process Improvement** – Shift from rigid, compliance-heavy models to agile, mission-driven acquisition. Replace JCIDS with capability-based assessments, use red teams for early security evaluation, improve market research, adopt open architecture, and consolidate cybersecurity frameworks. Enable faster, value-based procurement through modernized planning and fast-track lanes.
3) **Technology: Innovation and Cyber Resilience** – Distribute innovation responsibilities across mission offices. Evaluate DIU and CDAO, implement secure-by-design frameworks with SBOM/HBOM, require pre-award risk assessments, and establish a Risk Acceptance Governance Board. Monitor post-award supply chain security continuously.

4) **Cross-Cutting: Detecting and Preventing Foreign Influence** – Enforce continuous enterprise trust scoring and standardized FOCI disclosures. Mandate SBOMs and HBOMs for all critical systems to improve supply chain transparency and block adversarial influence.
5) **Small Business Enablement** – Simplify entry for small and non-traditional vendors. Create a centralized onboarding platform, establish a Small Business Innovation Liaison, and align SBIR/STTR programs with the Adaptive Acquisition Framework to accelerate transition to production.
6) Resilience and Risk Management – Reduce reliance on single vendors by formalizing lifecycle trust scoring, mandating modular procurement, and adopting multi-source strategies to enhance mission continuity and supply chain resilience.
7) Pilot-based Capabilities-Focused Acquisition – Minimize risk in the "Golden Dome for America" initiative by chartering a capabilities-focused pilot, "Project Discern." Leverage innovation entities like DIU to run a competitive bake-off that sources multiple, independent classifiers. Employ a voting ensemble and multiclass classification to support a human-on-the-loop workflow and mandate SBOM/HBOM for transparency.

People: Workforce Readiness and Cultural Transformation Recommendations:

- Foster a culture of innovation through mentoring and case studies.
- Realign workforce incentives toward secure innovation and timely delivery.
- Embed real-time threat intelligence within acquisition reviews.
- Modernize DAU training to include threat modeling and supply chain risk.
- Assign executive sponsors to high-priority procurements.
- Deploy Agile Tiger Teams of seasoned acquisition experts.
- Minimize reliance on legacy SETA contractors.

Rationale and Proposed Solutions:

Cultural transformation is essential for acquisition modernization. Currently, entrenched contractors and legacy processes stifle innovation, emphasizing compliance over agility. Realigning incentives toward secure innovation, updating DAU training to address contemporary threats and market realities, and providing mentoring through detailed case studies significantly increase workforce adaptability and effectiveness. Executive sponsors and Agile Tiger Teams further reduce bureaucratic barriers, improving responsiveness to mission-critical needs.

The root cause isn't just policy—it's the workforce mindset and incentive structure. Acquisition professionals are trained and rewarded based on compliance to outdated processes rather than on mission effectiveness, speed, or innovation. Inflexible frameworks like RMF are perpetuated by a lack of cross-trained talent and limited understanding of modern cyber risk management.

Despite well-intentioned reforms, such as the Adaptive Acquisition Framework (AAF), progress has been uneven because acquisition personnel are not equipped or incentivized to take advantage of agile, secure-by-design practices. Overreliance on SETA contractors further embeds legacy thinking, while DAU training has lagged in incorporating real-time threat intelligence, red teaming, or adversarial modeling.

The failure to empower and reform the acquisition workforce has resulted in systemic bottlenecks, degraded readiness, and unnecessary costs. This underscores the need to embed secure innovation metrics into performance reviews, integrate threat intelligence into acquisition processes, and retrain personnel through experiential learning and real-world case studies.

Transformation in defense acquisitions fundamentally depends on people and culture. Traditional SETA contractors often perpetuate outdated processes, limiting innovation. A mentoring-based culture paired with modernized training programs that focus on real-world threat modeling and supply chain risks empowers the workforce. Introducing incentives that reward innovation, rapid deployment, and security compliance ensures active participation in change management. Executive sponsors provide strategic oversight and accountability, ensuring mission alignment and rapid decision-making. Agile Tiger Teams further enhance responsiveness and expertise, ensuring acquisition agility.

Case Study:

The Risk Management Framework (RMF) remains an overly bureaucratic system that inhibits agility. In April 2024, Katie Arrington publicly called RMF "archaic," noting it can delay even simple changes for months. These delays are symptoms of a workforce trained to prioritize documentation over impact. Without reform in training, incentives, and leadership structure, such inertia will continue to undermine EO 14265's goals.

Process Improvement Recommendations:

- Transition to a mission-driven acquisition model aligned with agile commercial practices.
- Replace JCIDS with capability-based assessments aligned to robust market intelligence.
- Institutionalize acquisition red teams for early security evaluation.
- Reform Acquisition Planning and POM processes for better cost and performance transparency.
- Adopt open architecture principles, abandoning outdated DODAF.
- Consolidate duplicative cybersecurity frameworks (FedRAMP, ATO, CMMC).
- Create fast-track acquisition lanes for secure commercial products.

Rationale and Proposed Solutions:

Acquisition timelines are unnecessarily long due to outdated processes like JCIDS and poor market engagement. Legacy processes hinder timely capability delivery and limit flexibility in responding to rapidly evolving threats. Adopting agile methodologies, supported by robust capability assessments and interactive market research, enhances operational responsiveness.

Case Study:

The Air Force's Kessel Run initiative replaced traditional waterfall acquisition with agile software development methods. As a result, applications that previously took years to develop were delivered in months. This pivot to a mission-driven, iterative process model dramatically improved delivery speed, mission alignment, and user satisfaction. It also showed how legacy acquisition frameworks, like JCIDS, hinder responsiveness to operational needs, affirming the importance of replacing them with capability-based and market-informed assessments.

Technology: Innovation and Cyber Resilience Recommendations:

- Embed innovation responsibilities within all mission offices not isolated entities.
- Evaluate and restructure innovation units (DIU, CDAO) for operational integration.
- Mandate secure-by-design acquisition frameworks incorporating Cyber-Informed Engineering (CIE), zero-trust architectures, and mandatory Software and Hardware Bills of Materials (SBOMs/HBOMs).
- Require comprehensive pre-award risk assessments across personnel, hardware, software, and external dependencies.
- Establish a Risk Acceptance Governance Board to oversee security tradeoffs.
- Implement continuous post-award supply chain security monitoring.

Rationale and Proposed Solutions:

Executive Order 14265 represents a significant shift in defense procurement strategies. By prioritizing speed, flexibility, and commercial solutions, the order establishes a clear preference hierarchy that favors commercial off-the-shelf (COTS) products, followed by Other Transaction Authority (OTA) and Rapid Capabilities Office (RCO) policies. While this approach accelerates capability acquisitions and enhances responsiveness, it

reshapes the risk landscape by increasing dependency on commercial suppliers who may lack traditional security clearances and transparent supply chain processes, thereby heightening vulnerabilities such as adversarial infiltration, counterfeit components, and malware.

Innovation and cyber resilience must permeate every facet of defense acquisitions. Isolated innovation offices, without proper operational integration, limit overall effectiveness and resilience. Embedding secure-by-design and Cyber-Informed Engineering (CIE) principles into the acquisition lifecycle shifts risk management "left," proactively addressing cybersecurity threats rather than reacting post-incident. Comprehensive pre-award assessments and continuous operational monitoring further strengthen resilience, effectively mitigating risks posed by compromised supply chains and potential adversarial infiltration.

Case Study:

Innovation is often confined to standalone offices, reducing its operational impact. DISA's Zero Trust pilot, executed directly within a mission-focused agency, demonstrated measurable improvements in cyber resilience using secure-by-design frameworks. In contrast, siloed innovation offices like DIU often lack the authority or operational integration to drive change. The success of mission-embedded pilots highlights the need to embed innovation responsibilities across the acquisition ecosystem. Similarly, continuous supply chain monitoring and pre-award assessments would help mitigate threats like those exploited in the Volt Typhoon campaign.

Detecting and Preventing Foreign Influence Recommendations:

- Implement continuous enterprise trust scoring across critical acquisitions.
- Mandate SBOMs and HBOMs for critical technologies to ensure supply chain transparency.
- Standardize comprehensive FOCI disclosures.
- Develop tiered risk assessment protocols that distinguish between low-risk commercial acquisitions and critical defense systems

---

Rationale and Proposed Solutions:

Foreign influence represents a persistent threat to defense integrity. Current gaps in transparency and inconsistent disclosure practices have historically enabled adversarial infiltration. Mandating standardized disclosures and comprehensive bills of materials provides visibility necessary to detect and proactively mitigate threats, aligning with secure-by-design principles and reinforcing national security.

For commercial solutions, streamlined risk assessment protocols should incorporate NIST SP 800-161 guidelines for cybersecurity supply chain risks, including mandatory vendor due diligence focused on provenance tracking and threat-intelligence integration to mitigate foreign ownership, control, or influence (FOCI) risks. Particular attention must be paid to Information and Communication Technology (ICT) components, where SCRM extends beyond traditional security measures to include comprehensive supply chain provenance verification, ensuring that critical technologies are not sourced from adversarial nations that could embed malicious capabilities or create strategic dependencies.

Critical systems require comprehensive SCRM processes that address dependency on single-source suppliers, geopolitical risks, and supply chain vulnerabilities extending through multiple countries and potentially adversarial nations. The playbook's incident response and supply chain disruption protocols become even more important under this accelerated approach, as increased reliance on commercial suppliers may create new vulnerabilities requiring rapid response capabilities.

Addressing foreign influence is paramount in protecting national security. Continuous, proactive trust scoring enables early detection and intervention, significantly reducing vulnerabilities. Mandating SBOMs and HBOMs for critical systems creates transparency and traceability, critical for identifying compromised components. Standardized FOCI disclosures across acquisition tiers enhance scrutiny and mitigate foreign influence effectively.

Case Study:

Lack of transparency in software supply chains has led to major national security breaches. The SolarWinds compromise exploited invisible software dependencies. Had SBOMs and trust scoring been mandatory, this threat could have been identified pre-deployment. Likewise, FOCI disclosures remain inconsistent, enabling adversarial ownership in critical systems. These gaps must be closed.

Small Business Enablement Recommendations:

- Establish a Small Business Innovation Liaison to guide vendors through compliance and security requirements.
- Align SBIR/STTR programs with Adaptive Acquisition Framework to ensure smoother transition from prototype to production.

- Develop a centralized digital onboarding platform to reduce compliance complexity for small businesses.

Rationale and Proposed Solutions:

Small and non-traditional vendors are essential to defense innovation but face disproportionate barriers. Establishing streamlined support and alignment through a dedicated liaison and centralized resources reduces entry friction, enabling small businesses to rapidly contribute innovative, secure technologies within the defense industrial base.

Case Study:

CMMC compliance costs disproportionately burden small businesses, with Level 2 assessments alone exceeding $100,000. A centralized digital onboarding platform, along with dedicated Small Business Innovation Liaisons and better alignment of SBIR/STTR programs, could dramatically lower these costs and streamline compliance, significantly enhancing small business capabilities and contributions to defense innovation.

Resilience and Risk Management Recommendations:

- Formalize lifecycle risk scoring frameworks to assess vendor dependencies.
- Mandate modular procurement and multi-source strategies to mitigate single-point failures.
- Create resilience benchmarks and contingency plans addressing supply chain disruptions.
- Develop a DoD-wide Risk Management Playbook incorporating threat intelligence, dependency mapping, and impact analyses.

Rationale and Proposed Solutions:

Over-reliance on singular vendors and proprietary solutions undermines mission continuity. Formalized lifecycle assessments, modular procurement, and contingency planning ensure agility, adaptability, and continuity in face of disruptions. Systematic integration of CIE ensures these approaches inherently prioritize cybersecurity, enhancing overall resilience.

Case Study:

The JEDI Cloud program was canceled after protests revealed a dependence on a single provider that posed both strategic and legal risk. Future cloud or software procurements should not hinge on single-point dependencies. Mandating modular, multi-vendor architectures and up-front dependency risk analysis would prevent systemic lock-in and strengthen mission continuity. This principle applies broadly—from tactical edge devices to national command platforms.

Action Plan and Pilot Recommendations

- To rapidly advance the goals of Executive Order 14186, charter a pilot program, Project Discern, under the Middle Tier of Acquisition (MTA) for Software authority. This pilot must be structured around a capabilities-focused challenge rather than a traditional requirements document, rewarding vendors for delivering effective outcomes.
- Task a specialized organization from the DoD Innovation Ecosystem, such as the Defense Innovation Unit (DIU), to lead and execute Project Discern, leveraging its expertise in rapid prototyping and commercial technology integration.
- Direct the selected organization to prepare an out-of-cycle issue paper to secure the necessary funding through reprogramming actions, justifying the immediate allocation of resources to this presidential-level initiative.
- Direct a DoD Laboratory or a Federally Funded Research and Development Center (FFRDC) to create and maintain the authoritative datasets for the competition. These datasets must include a robust mix of real-world and synthetically generated data, encompassing both tagged (labeled) and untagged examples to test supervised and unsupervised learning approaches.
- Structure the pilot as a competitive "bake-off" to source multiple, independently developed classifiers from a wide range of vendors, ensuring a diversity of algorithmic approaches.
- Implement a voting ensemble framework that integrates the top-performing independent classifiers, using their combined outputs to generate a final, robust classification.
- Design the system's output to sort detected objects into categories such as Hostile Threat, Potential Threat/Uncertain, Non-Threat, and Known Civilian/Safe.
- Build the system's interface to explicitly support a human-on-the-loop (HOTL) workflow, ensuring that ambiguous or conflicting classifications are flagged for immediate operator judgment.
- Mandate that each selected solution be delivered with complete Software and Hardware Bills of Materials (SBOMs/HBOMs) to ensure full transparency and security.

Rational and Proposed Solutions:

Achieving the national-scale defense envisioned by EO 14186 is impossible using traditional, requirements-driven acquisition models that are too slow and rigid. The algorithmic core of such a system—its ability to discriminate between thousands of objects in a cluttered domestic airspace—represents its most complex and highest-risk component. This pilot shifts the

paradigm by presenting industry with a capabilities-focused challenge, incentivizing innovative solutions to a complex problem rather than mere compliance with a static list of specifications. As the Nation invests in the immense physical infrastructure of an "Golden Dome for America" it is essential to first prove and de-risk this critical decision-making engine, as is being offered by the IT-AAC's Tech Proving Ground initiated by DIU.

Project Discern should pair two powerful concepts: multiclass classification and an ensemble of independently developed models. Sourcing classifiers from different teams ensures a diversity of thought in the algorithms themselves. This approach is essential for a national system for two reasons:

1. High-Confidence Consensus: If different, independently developed models all arrive at the same conclusion (e.g., "Hostile Threat"), it provides an exponentially higher degree of confidence—a prerequisite for any system defending the homeland.
2. Disagreement as Data: If the models disagree, that conflict is itself a critical piece of information. It acts as an automated "sanity check," immediately flagging the object as "Potential Threat/Uncertain" and elevating it for human-on-the-loop review. This is not a bug, but a feature, ensuring a human is involved in ambiguous cases.

This architecture or close variations are the only responsible way to build the trusted foundation required to fulfill the mandate of Executive Order 14186.

Case Study:

The catastrophic downing of Iran Air Flight 655 by the USS Vincennes in 1988 illustrates the profound risks of misclassification. Now, imagine that risk scaled to the level of an "Golden Dome for America," which must operate flawlessly within a domestic airspace containing thousands of commercial, cargo, and private aircraft at any given moment. A single error would be a national tragedy. The lesson from the Vincennes is clear: a system's ability to avoid error is as important as its ability to intercept threats.

A system built according to the principles of Project Discern would address this risk head-on. An ensemble of independent models would likely have produced a split decision on Iran Air 655, forcing a deliberate human review instead of allowing for a single point of failure. The responsible implementation of Executive Order 14186 demands this level of analytical rigor and safety. We must validate and harden the system's judgment before we build its walls.

Conclusion

EO 14265 presents a rare opportunity to modernize DoD acquisition at a systemic level. We urge DoD to implement these recommendations—especially the replacement of outdated processes, the alignment of workforce incentives, and the detection of foreign influence—through enforceable

reforms rather than voluntary measures. We welcome the opportunity to support this transformation by contributing to working groups, pilot programs, or targeted implementation efforts.

The success of Executive Order 14265's implementation will largely depend on how effectively defense organizations can integrate SCRM principles into accelerated acquisition processes without viewing speed and security as competing priorities. Rather than compromising oversight in pursuit of agility, organizations must leverage systematic SCRM approaches to build security considerations into streamlined workflows. This integration ensures that defense industrial base modernization strengthens rather than compromises the overall security posture of defense supply chains.

By proactively addressing supply chain risks (SCRM) and trustworthiness, through enhanced supplier risk assessments, continuous monitoring protocols, and robust governance mechanisms, the Department of Defense can achieve the "peace through strength" objective of EO 14265 while maintaining the supply chain risk management capabilities essential for protecting national security interests in an increasingly complex global threat environment. The ultimate goal is fostering innovation without inviting exploitation, creating a defense industrial base that is both agile and secure.

We welcome an opportunity to discuss in greater detail.

John A. Weiler
Executive Director - CoFounder, IT Acquisition Advisory Council (john.weiler@IT-AAC.org)
CEO, Interoperability ClearingHouse (ICHnet.org) a DOD chartered nonprofit research institute
CTO Army Partnership Intermediary Agreement https://www.newswire.com/news/army-research-lab-signs-partnership-intermediary-agreement-pia-with-22585494
Member, Congressional DOGE Caucus (Ernst)
Vice Chair, Cloud Safe Task Force (Mitre, ATARC, CSA, IT-AAC)
Member, DHS CISA ICT SCRM Task Force
Partner, Technology Advancement Center (formerly MISI)
Founding Member, CMMC Accreditation Board (Nov 2019-July 2020)
US Public Sector Director, TBM Council (TBMCouncil.org)
Linkedin: linkedin.com/in/joweiler
Twitter handle: @johnaweiler
703-863-3766 (M)
Defense IT Reform Podcast with NDIA https://www.youtube.com/watch?v=7xN4xtM4qI0&t=15s
My view on fair/open competition on Newsweek; vid.newsweek.com/why-competition-important-when-pentagon-buys-technology-560248