



CREATIVE DEFENSE FOUNDATION

SUMMARY REPORT

NSPPC INAUGURAL CONVENING

National Security Prototype to Production OT Consortium

St. Paul RiverCentre · Saint Paul, Minnesota • 18 September 2026



NSPPC



THE NATIONAL SECURITY PROTOTYPE TO PRODUCTION OT CONSORTIUM
FRIDAY, SEPTEMBER 18, 2026 • 8:00 AM - 12:00 PM • SAINT PAUL RIVERCENTRE

IN THIS REPORT

SESSIONS

FRIDAY, 18 SEPTEMBER 2026

01	Welcome Remarks	OPENING REMARKS
02	NSPPC Opening	KEYNOTE REMARKS
03	Introducing the NSPPC	FIRESIDE CHAT
04	Organization Governance of Plug-and-Play Ecosystems	PANEL DISCUSSION
05	Incentivizing Multi-Vendor Integration at Scale	PANEL DISCUSSION
06	Rebuilding the National Security Industrial Base	FIRESIDE CHAT



01

OPENING REMARKS

WELCOME REMARKS

SESSION OVERVIEW

The Chair of the Minnesota National Security Ecosystem kicked off the sixth Creative Disruptors conference in St. Paul, Minnesota, bringing together congressional representatives, senior military officials, and private sector leaders to address pressing national security challenges. Hosted by the Creative Defense Foundation (CDF) in partnership with the Minnesota National Security Ecosystem, the event represents the third conference held in Minnesota alongside three prior iterations in California.

The Chair recognized the founders and Executive Director of the Creative Defense Foundation for establishing the platform. He also welcomed congressional co-hosts, including House Defense Appropriations leadership and a member of the Minnesota congressional delegation. Together, they delivered opening remarks focused on the following three themes.

LAUNCH OF PROTOTYPE TO PRODUCTION CONSORTIUM

A primary focus of the opening remarks was the official launch of the **National Security Prototype to Production Consortium (NSPPC) for Plug-and-Play Composable Warfighting**. Developed by CDF in partnership with the Department of Defense and the U.S. Navy, the consortium provides a structured mechanism to accelerate the transition of critical technologies from initial prototypes into scaled procurement. Defense leaders emphasized that establishing interoperable standards and reducing adoption timelines are essential steps toward modernizing equipment for military personnel.

EXPANSION OF THE REGIONAL DEFENSE ECOSYSTEM

Speakers highlighted the growth of Minnesota and the broader Great Lakes region as an expanding base for defense innovation. While regional contributions to the national defense enterprise have historically trailed other areas, localized coordination among entrepreneurs, research entities, and industrial partners has accelerated in recent years. Expanding this five-state ecosystem aims to connect regional commercial capabilities with federal security needs, driving regional economic growth and workforce development.

STRATEGIC AND LEGISLATIVE PRIORITIES

Legislators underscored the requirement to move beyond standard acquisition practices to maintain long-term strategic readiness. Pointing to the complementary roles between House authorizing and appropriating committees, lawmakers stressed the importance of bipartisan cooperation in funding and executing defense technology initiatives. The conference agenda centers on converting industry dialogue into operational policy, focusing on the convergence of software, hardware, and advanced technology to address global competitive threats.



02 KEYNOTE REMARKS NSPPC OPENING

SESSION OVERVIEW

The Founder and Chairman of the Creative Defense Foundation (CDF) formally opened the **National Security Prototype to Production Consortium (NSPPC)** working session in St. Paul, Minnesota. He acknowledged key event organizers and production leaders, including CDF's co-founder, CDF staff members, and Kate Taylor Events, and highlighted the attendance of senior military leaders, agency secretaries, and the dean of the Minnesota congressional delegation, representing 800,000 area residents. His remarks established the strategic rationale for the consortium, tracing its roots from small business statutory reforms to modern AI-driven integration architectures.

AI AVATARS AND THE NSPPC FRAMEWORK

The opening featured updated digital versions of **Entra** and **Intra**, AI avatars representing "entrepreneurial" and "intrapreneurial" innovation that have served as CDF spokespersons for three years. In a presented video segment, the avatars outlined the transition from previous operational demonstrations, such as a multi-vendor kill chain exercise at a prior Disruptors in the Desert conference, to establishing the NSPPC in partnership with the Department of the Navy. Framed as a high-occupancy vehicle (HOV) fast lane designed to bridge the traditional defense acquisition "valley of death," the consortium provides non-traditional contractors, innovators, and prime vendors a direct path from initial prototype to scaled production. The Chairman also explained the symbolism of the CDF logo, where individual dots represent raw concepts and connecting lines represent prototypes plugging directly into the national security enterprise.

SBIR STATUTORY REFORM AND LESSONS IN ACQUISITION

The Chairman grounded the consortium's mission in his background as a defense entrepreneur founding Digital System Resources (DSR), an underwater acoustics firm focused on submarine sonar capabilities. After initial funding through Phase I and Phase II Small Business Innovation Research (SBIR) grants, he encountered statutory requirements that mandated open competitions for Phase III follow-on contracts, effectively forcing founders to compete against outside firms for their own developed technology. In response, he formed the Small Business Technology Coalition and successfully engaged Congress to amend acquisition law, establishing that Phase I and Phase II awards satisfy the Competition in Contracting Act for Phase III transition. DSR subsequently grew into a top 100 U.S. defense research firm before its acquisition by General Dynamics in 2003, illustrating that creating viable acquisition pathways is as critical as developing the technology itself.

THE INTEGRATED ARSENAL FOR DEMOCRACY

Addressing current security conditions, the Chairman emphasized that unmanned systems, drones, and artificial intelligence multipliers are fundamentally altering military capabilities and homeland defense requirements. Building effective defense capability requires moving beyond manufacturing isolated hardware platforms to developing interoperable sensors, communications, software, and mission payloads. Achieving an "integrated arsenal for democracy" demands plug-and-play composability where separate commercial products connect through standardized interfaces, establish performance trust, and integrate seamlessly into active operations.

AI-DRIVEN SYSTEMS INTEGRATION AND COMMERCIAL GOVERNANCE

Artificial intelligence serves as a tool for system-level integration by automating complex engineering tasks, including comparing hardware interfaces, reconciling disparate data formats, and testing component interoperability at scale. Under a formal Memorandum of Agreement with the Department of War, CDF interacts directly with federal agreements officers to execute consortium activities alongside partners such as the Navy Rapid Capabilities Office. To structure these interfaces without penalizing competing firms, the consortium incorporates governance principles from established commercial ecosystems, such as telecommunications networks, the internet, and human genome mapping, allowing technologies to evolve while preserving participant business models.

INDUSTRY ENGAGEMENT AND PROGRAMMATIC NEXT STEPS

The Chairman's opening remarks concluded with an outline of upcoming conference programming designed to facilitate peer-to-peer engagement and industry coordination. He highlighted an upcoming technology exhibition featuring 30 commercial vendors displaying plug-and-play solutions.



03

FIRESIDE CHAT

INTRODUCING THE NSPPC

SESSION OVERVIEW

The NSPPC's first fireside chat examined the operational execution of the National Security Prototype to Production Consortium (NSPPC), detailing its mission architecture, commercial benchmarks, and technology transition mechanisms.

The conversation traced the historical development of the consortium concept, outlined a structured framework for problem decomposition, and detailed the integration of digital simulation tools.

ORIGINS AND INSTITUTIONALIZING PLUG-AND-PLAY

The concept for the NSPPC emerged from multi-year strategic discussions focused on moving defense gatherings beyond networking and toward actively shaping the industrial base. Plug-and-play capability development within the Department of Defense builds on initial efforts started with the Strategic Capabilities Office in 2020. The Navy's Rapid Capabilities Office is currently in its second year of institutionalizing this framework service-wide, aiming to deliver specialized capabilities with speed and effectiveness outside traditional multi-decade procurement efforts like aircraft carriers or major fighter aircraft.

MISSION ENGINEERING AND PROBLEM DECOMPOSITION

Effective acquisition requires analyzing joint operational problems through rigorous mission engineering before attempting solution synthesis. Under current reform efforts within the Office of the Assistant Secretary of War for Mission Capabilities, complex defense challenges and kill chains are broken down into discrete technical requirements, performance measures, and operational parameters. Sharing these detailed metrics across digital platforms allows commercial developers to understand exact military needs rather than trying to divine government requirements independently.

THE 80 PERCENT COMMERCIAL SOLUTION MODEL

To avoid delays caused by long development cycles and overly rigid specifications, acquisition strategies prioritize identifying existing commercial capabilities that offer an 80 percent solution. In areas like radio frequency engineering and commercial transmitters, vendors do not require high-level security clearances to provide functional hardware. Instead, government program offices break down classified requirements into unclassified technical parameters, allowing commercial entities to present existing technologies that the military can then adapt or integrate into broader mission architectures.

ADDRESSING THREAT AND SOLUTION VELOCITIES

Modern defense procurement must manage two distinct rates of change: the rapid evolution of adversary threats and the frequent turnover of which commercial entity holds the optimal technical solution. Bespoke vertical integrations are unable to keep pace with these dual velocities. To address this, the NSPPC utilizes industry-led committees that establish, maintain, and adapt technical interfaces and open standards. This industry-facing structure allows new commercial innovators to plug into existing defense systems without requiring full-system redesigns.

COMMERCIAL ECOSYSTEM BENCHMARKS

The consortium draws governance and architectural lessons from non-defense technical ecosystems, including the internet, commercial telecommunications networks, and the human genome mapping project. In commercial networks, new hardware like Wi-Fi routers can be integrated seamlessly without retesting the broader internet infrastructure. Similarly, mapping the human genome provided a government-funded foundational architecture that commercial pharmaceutical firms build upon. Applying these principles to defense acquisition establishes clear business models for industry while protecting proprietary intellectual property.

DIGITAL TWINS AND SYNTHETIC MISSION TESTING

Accelerated fielding relies on a "build it twice" methodology, where technologies are constructed and validated in a virtual environment before undergoing physical manufacturing. Drawing inspiration from past initiatives like DARPA's Assault Breaker II program, current mission engineering efforts employ multi-cloud, multi-classification digital platforms to model scenarios, distribute tools, and integrate artificial intelligence. This synthetic approach compresses analysis timelines from years down to days or weeks, confirming that digital twins deliver required mission-level effects before capital is committed to physical scale.

SUSTAINABLE BUSINESS MODELS AND CONTINUOUS FIELDING

Achieving long-term value for both taxpayers and warfighters requires translating mission analysis into sustainable, five-year funding projections across programming elements. Clear demand signals give commercial partners the confidence needed to scale production capacity. Furthermore, rather than treating procurement as a single static delivery, the consortium framework supports continuous, iterative releases that directly address real-time operational feedback from frontline personnel.



04

PANEL DISCUSSION

ORGANIZATION GOVERNANCE OF PLUG-AND-PLAY ECOSYSTEMS

SESSION OVERVIEW

The NSPPC's first panel discussion evaluated how defense acquisitions can adopt organizational governance models from successful commercial technical ecosystems, such as 3GPP, O-RAN, and OpenAPI.

The discussion emphasized that effective plug-and-play frameworks require neutral stewardship, dynamic standards management, and automated conformance testing to align thousands of competing suppliers without creating technical monopolies. To illustrate how this governance functions in practice, the panel examined the breakdown of legacy standards, the creation of live software marketplaces, direct industry gauntlets, test infrastructure expansion, and the realignment of acquisition to supply chain models.

LEGACY META-STANDARDS AND TECHNICAL OVER-SPECIFICATION

Government acquisition historically over-prescribes detailed hardware implementations rather than defining functional mission outcomes, akin to dictating the physical size and shape of automobile taillights rather than their operational brightness. While baseline standards such as 3GPP, TCP/IP, JSON, and OpenAPI drive global commercial technology, defense programs frequently overlay proprietary meta-standards that introduce rigidity. A prime example is the requirement for modern systems to maintain backward compatibility with legacy tactical networks like Link 11, which

traces its roots to mid-twentieth-century architectures, alongside Link 16. In one exercise, legacy message formats passing between service systems produced a track misclassification, and certification hurdles, authority-to-operate constraints, and rigid test baselines prevented engineers on-site from modifying the software, demonstrating how rigid standardization blocks necessary operational adjustments.

DIGITAL INTERFACES, API MARKETPLACES, AND OPERATION JAILBREAK

The Department of War is replacing static paper interface documents with dynamic, machine-readable interface descriptions utilizing REST, gRPC, RPC, and Swagger protocols. Initiated by Army leadership to eliminate paying vendors repeatedly to connect existing systems, Operation Jailbreak created an unclassified API Marketplace accessible at marketplace.dso.mil. During an initial six-week sprint at Fort Carson involving 70 vendors and 80 systems, followed by a theater-support sprint in Tampa encompassing 70 vendors and 102 systems, participants achieved a 100 percent integration completion rate. The process enabled autonomy competitions that moved from solicitation to contract award in 128 hours, with capabilities deployed to an operational division for assessment within nine days. Prime contractors, including Lockheed Martin and Raytheon, exposed gRPC interfaces for platforms such as the Sentinel, KURFS, and TPQ-53 radar sensors without compromising proprietary intellectual property.

JOINT SERVICE CONVERGENCE AND DIGITAL ACQUISITION

Rather than establishing separate service-specific initiatives, Navy, Marine Corps, and CENTCOM personnel joined the Army's Jailbreak framework to ensure joint operational interoperability. Service leadership now evaluates pilot programs on three- to four-month cycles, scaling successful concepts or terminating underperforming efforts rapidly. In aviation and autonomous systems acquisition, program offices are replacing traditional 300-page written proposals with digital engineering models. Proposals are evaluated directly within synthetic environments, establishing interoperability as a core selection metric and allowing defense buyers to assess edge economics and autonomous behaviors before issuing production contracts.

DRONE DOMINANCE, GAUNTLET TESTING, AND MARKET-DRIVEN STANDARDS

The Drone Dominance pilot program bypasses multi-year Joint Requirements Oversight Council approval processes, transitioning from initial concept to an industry call within 30 days and executing live field tests 30 days later. Following initial evaluations at Fort Benning, the program introduced Camp Grayling regional qualifiers modeled after professional sports tournaments, inviting top-performing vendors to Gauntlet 2 at Fort Custer. During Gauntlet 2, 26 commercial companies operated autonomous systems against active electronic jamming and JIATF 401 counter-UAS platforms. A subsequent Gauntlet 2.5 event was added specifically to evaluate bomber drone configurations. Test results and performance rankings are published directly to a public online leaderboard at drones.mil, accessible for procurement by federal, state, local, and tribal government entities. When a drone lost power due to a disconnected battery during flight testing, the program issued a zero score rather than drafting a costly military-specification connector, driving industry competitors to establish reliable interface standards independently.

TESTING INFRASTRUCTURE, INNOVATION RANGES, AND LIVE-FIELDING VALIDATION

Organic military test facilities like White Sands, Edwards, and Eglin Air Force Base face severe throughput constraints and risk-averse protocols. For instance, a vendor that tested a new platform rapidly at a private range encountered substantial administrative delays when transitioning to traditional military range testing. To solve this, the Test Resource Management Center is establishing Innovation Ranges at National Guard sites and public-private locations in Huntsville,

Mississippi, Camp Grayling, and overseas sites in Morocco. These sites form a minor-league testing pipeline where commercial data remains valid for formal acquisition. In parallel, tactical units are conducting early live stress testing, such as the 2nd Cavalry Regiment's Flytrap exercise in Europe, which integrated Helsing software and counter-UAS hardware under active soldier usage and electronic warfare duress.

AUTOMATED INTEGRATION, CROSS-DOMAIN REFORM, AND PORTFOLIO ACQUISITION

Modernizing acquisition requires shifting software validation left through automated testing tools, such as those developed by Innovative Defense Technologies, enabling continuous mission-level simulation without multi-month certification delays. Defense programs are actively eliminating cross-domain translators, cutouts, and stitched interfaces that hide rich data inside legacy formats like Cursor on Target XML. In place of static net-ready metrics, programs now mandate software adaptability, as demonstrated by Covenant missile testing during Project Convergence. Ultimately, mission engineering is being reframed as an end-to-end supply chain problem where the final delivered product is an operational effect. Transitioning management into Portfolio Acquisition Elements allows program executive officers to decommission obsolete systems, reallocate capital, and eliminate the multi-year process delays that traditionally add significant cost overhead to defense procurement.



05

PANEL DISCUSSION

INCENTIVIZING MULTI-VENDOR INTEGRATION AT SCALE

SESSION OVERVIEW

The NSPPC's second panel discussion evaluated strategies for incentivizing multi-vendor integration at scale, focusing on converting Modular Open Systems Approach (MOSA) principles into fielded combat capability.

. Multi-vendor kill chains require aligning commercial business models, establishing data standards, and resolving cross-organizational dependencies across the defense enterprise. To understand how the Department of War and industry intend to operationalize these concepts, the discussion outlined detailed friction points and solutions across software architecture, prime contractor economics, bureaucratic implementation gaps, supply chain scheduling, data valuation, and consortium governance.

LEGACY ARCHITECTURAL ABSTRACTION AND DATA ROUTING BOTTLENECKS

Integrating modern commercial software with military hardware requires bridging two distinct technological generations. Legacy defense systems rely on outdated data architectures and standards dating back to 1957, such as Link 11, which feature incompatible ontologies and user interfaces. Because wholesale system replacement is impractical during active global conflicts, current strategy focuses on extracting flawed user interfaces and capacity bottlenecks while layering modern data platforms over existing infrastructure, effectively renovating the user-facing

capability while leaving foundational plumbing intact. In current operational kill chains, poor data architecture frequently causes a single data packet to bounce between cloud and on-premise servers seven times across the country before reaching command-and-control operators, driven by vendor silos and legacy on-premise architectures.

PRIME CONTRACTOR ECONOMICS AND PERFORMANCE REQUIREMENTS

Lead System Integrator (LSI) business models frequently disincentivize sub-tier vendor integration. Bringing on additional subcontractors reduces gross profit margins and increases administrative overhead, prompting major prime contractors to bring development in-house to maintain quality control, manage parts qualification, and protect profit margins. Furthermore, traditional procurement penalizes test failures by canceling programs rather than iterating on lessons learned. Shifting acquisition from rigid, specified requirements toward performance-based mission requirements, coupled with monetary incentives tied to speed, cost reduction, and multi-vendor integration, aligns corporate profit structures with rapid capability composition.

THE MIDDLE-MANAGEMENT BUREAUCRACY AND READINESS GAPS

A significant implementation gap exists between high-level policy and program execution. While strong alignment exists among Congress, defense undersecretaries, and service acquisition executives, middle-management civil servants and program managers frequently reframe modern software, data, and standards concepts using legacy bureaucratic definitions. This institutional friction slows fielding while adversaries innovate rapidly with lower-cost, highly effective systems. Readiness suffers as a result, with the operational availability of key platforms constrained by basic component shortages. Furthermore, federal procurement currently utilizes only 35 percent of available industrial base capacity in regions like the Upper Midwest due to outdated vendor discovery processes.

DISAGGREGATED SUPPLY CHAINS AND "LAUNCH CHICKEN" SCHEDULING

The defense industrial base operates as isolated organizational nodes that lack continuous digital communication threads, relying heavily on manual spreadsheets, emails, and static slide decks. This lack of real-time visibility produces systemic scheduling delays, exemplified by the "launch chicken" phenomenon in the space sector where satellite developers and rocket launch providers conceal schedule slips until weeks before launch. These scheduling and integration disconnects contribute directly to major program budget overruns and operational delays. Utilizing self-hosted, hardened artificial intelligence to ingest real-time project data across vendors and program offices allows defense managers to identify cross-boundary behavioral bottlenecks and schedule delays well before they cause cost overruns.

REINTERPRETING INTELLECTUAL PROPERTY AND DATA VALUATION

Intellectual property represents the core commercial valuation for defense vendors, making forced IP surrender a major point of friction. Contractor firms guard historical test data to prevent competition, while government program offices frequently negotiate for broad IP rights only to store proprietary information unread on closet hard drives. Effective data governance requires structured business relationships where government authorities negotiate monetary price discounts when data rights are unnecessary, or establish dynamic usage agreements, anonymization protocols, and accessible application programming interfaces (APIs). In software-defined warfare, data quality defines capability, making traceable ontologies and metadata enforcement essential alternatives to rigid, single-ontology mandates.

OPERATIONAL CASE STUDIES IN RAPID INTEGRATION

To demonstrate how modular open-systems concepts and data-centric architectures function in practice, panelists highlighted several operational proofs of concept. These case studies illustrate how automated testing, decoupled software layers, and dynamic data utilization can bypass traditional procurement bottlenecks to deliver rapid capability improvements across hypersonic development, tactical logistics, and battle management systems:

- **TRMC Scramjet Testing:** Working with the Test Resource Management Center, North Wind trained AI algorithms on six months of historical wind tunnel data. Automated testing in wind tunnels identified flow anomalies in real time and adjusted parameters automatically, compressing a traditional four-to-six-month anomaly test cycle down to three days.
- **Fort Snelling Logistics Tracking:** National Guard units near St. Paul deployed plug-in software platforms over existing logistics data to track armaments, medical supplies, and equipment in real time, establishing a model for commercial software integration.
- **Army NGC2 Architecture:** The Army Next Generation Command and Control program implemented a decoupled application layer and data layer where no vendor maintains permanent job security, establishing a plug-and-play environment where underperforming software applications can be swapped out seamlessly.

NSPPC FRAMEWORK, COMPOSABILITY DECLARATIONS, AND GOVERNANCE

The moderator closed the panel discussion highlighting the critical need to operationalize multi-vendor integration. He elaborated that the National Security Prototype to Production Consortium (NSPPC) operates under a Department-wide Memorandum of Understanding (MOU) managed by the Creative Defense Foundation (CDF), allowing any agreements officer across the Department of War to execute awards. Bidding vendors submit digital "composability declarations" alongside technical proposals, providing AI agents, data files, interface ontologies, and behavioral models that detail exactly how their hardware and software plug into the broader ecosystem. The consortium supports a shared Mission Integration Commons in coordination with the Creative Defense Network, providing industry partners with access to test routines, data layers, and integration tools supported by dedicated leadership.



FIRESIDE CHAT

06

REBUILDING THE NATIONAL SECURITY INDUSTRIAL BASE

SESSION OVERVIEW

The NSPPC's second fireside chat evaluated federal strategies for rebuilding the defense industrial base to ensure long-term resilience, commercial scalability, and technology interoperability.

The discussion detailed official ingestion channels, technology priority lists, certification overhauls, and capital security requirements.

DIGITAL INGESTION, TECHNICAL HEAT-MAPPING, AND FINANCIAL VETTING

To streamline how commercial vendors present capabilities to the Department of War, research and acquisition offices have established digital front-door portals designed to bypass traditional bureaucratic delays. Commercial contractors can submit white papers and technical abstracts directly into these portals, where automated software agents scrape technical data to heat-map capabilities against active operational requirements across military branches:

- **Research and Engineering Portals:** Managed under the Critical Technologies portfolio (transitioning intake functions through the Defense Technical Agency), white paper submissions are evaluated using automated heat-mapping tools, with senior officials targeting a formal two-week technical feedback window.
- **Integrated Financial Reviews:** Submissions undergo simultaneous financial and technical assessments supported by embedded experts from In-Q-Tel and the Office of Strategic Capital to evaluate venture capital structures, private equity backing, and manufacturing scaling capacity.
- **Industrial Base Access Points:** Industrial Base Policy utilizes the Connect.io platform alongside Apex Accelerators, which engaged 26,000 companies in the preceding year to generate \$65 billion in defense revenue, complemented by the cornerstone OTA and DIPC OTA contracting vehicles.

PRIORITY TECHNOLOGY INITIATIVES AND SUPPLY CHAIN INVESTMENTS

Department leaders highlighted active capital deployments designed to field advanced capabilities while stabilizing lower-tier commercial supply chains. The Department is combining top-down demand signals with bottom-up raw material investments to ensure manufacturing lines can scale during multi-domain conflicts:

- **Contested Logistics and Directed Energy:** Critical technology priorities include fielding micro-reactors at the Naval Surface Warfare Center to deliver mobile power by September 2028 under executive order, transitioning joint laser weapon systems and high-power microwaves to the Army, and scaling the Microelectronics Commons to integrate updated chips into legacy hardware.
- **Raw Materials and Long-Term Contracts:** Industrial Base Policy has deployed nearly \$1.9 billion from the Industrial Base Fund into MAC programs while securing critical mineral supply chains, specifically targeting domestic processing for germanium, gallium, and rare earth elements.
- **Skilled Trades Workforce Expansion:** Through the "Build Freedom" initiative partnered with the mikeroweWORKS Foundation, the Department is investing over \$300 million, including \$10 million in dedicated scholarships, to expand skilled trade training programs from 40 to 70 sites nationwide.

ACQUISITION REFORM AND CERTIFICATION MODERNIZATION

Accelerating technology delivery requires pairing expanded statutory authorities with an aggressive overhaul of legacy administrative regulations. Backed by a \$850 billion base budget and a broader \$1.5 trillion total budget request incorporating supplemental funding, the Department is leveraging 2026 National Defense Authorization Act (NDAA) multi-year procurement authorities to establish stable demand signals for new market entrants:

- **Policy Barrier Removal:** Research and Engineering barrier removal boards are actively rescinding obsolete regulations, including multi-decade-old excluded technology lists that restrict commercial component usage.

- **Overhauling Qualification Protocols:** Testing and qualification directives built during the Cold War are being rewired to give commercial vendors greater ownership over certification testing, eliminating long-standing single-source vulnerabilities.
- **Resolving Legacy Supply Single Points:** Officials highlighted historical failure modes, such as the North American Round Corporation remaining the sole qualified provider for critical components three decades after ceasing operations in 1997 due to an unaddressed government lifetime buy.

ADVERSARIAL CAPITAL RISKS AND DIRECTIVES FOR INDUSTRY

The session concluded with direct operational guidance for commercial firms seeking to enter the defense ecosystem, emphasizing supply chain transparency and capital table integrity. Department officials cautioned that foreign adversarial capital represents an existential threat to commercial defense entrants equal to intellectual property theft:

- **Cap Table Vetting:** A meaningful share of commercial technology companies reviewed by defense offices have been found to have hidden connections to adversarial foreign capital, making comprehensive beneficial ownership audits mandatory across all investment rounds and regional venture funds.
- **Sub-Tier Supply Chain Audits:** Prime contractors and innovators must inspect Tier 2, Tier 3, and Tier 4 suppliers directly to identify scale bottlenecks and qualify second sources early, rather than concealing supply chain disruptions until operations break down.
- **Commercial Solution Ingestion:** Acquisition offices are actively seeking 75 to 80 percent "good enough" commercial solutions that can be fielded and iterated rapidly, urging vendors to bring operational challenges to light early and proceed without waiting for rigid government permissions.

