wiley

ALERT

What Contractors Need to Know About DOD's National Defense Industrial Strategy

January 19, 2024

WHAT: On January 11, 2024, the U.S. Department of Defense (DOD) published its National Defense Industrial Strategy (NDIS). In line with DOD's continued emphasis on modernizing and strengthening the supply chain and acquisition process, the NDIS seeks to "catalyze generational change from the existing defense industrial base to a more robust, resilient, and dynamic modernized defense industrial ecosystem." To address national security risks from inadequate domestic production for DOD-specific operations, reliance on foreign adversaries for critical materials, and procurement cycle instabilities, the NDIS focuses on four main areas of development: flexible acquisition, economic deterrence, resilient supply chains, and workforce readiness.

WHAT THIS MEANS FOR INDUSTRY: Although the NDIS does not advocate for broad acquisition reform or significant new legislation, it does identify a number of acquisition-related initiatives to achieve certain policy goals using existing acquisition authorities.

Prioritizing Flexible Acquisition

The NDIS places an emphasis on employing "flexible acquisition strategies" to improve its efficiency in acquiring innovative commercially available off-the-shelf capabilities (COTS), reducing costs of procurement, and enhancing production capabilities that strengthen the nation's supply chains.

DOD's emphasis on the use of flexible acquisition opportunities includes:

Authors

Tracye Winfrey Howard
Partner
202.719.7452
twhoward@wiley.law

Kevin J. Maynard
Partner
202.719.3143
kmaynard@wiley.law

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Hon. Nazak Nikakhtar
Partner
202.719.3380
nnikakhtar@wiley.law

Vaibhavi Patria
Associate
202.719.4667
vpatria@wiley.law

Lisa Rechden
Associate
202.719.4269
lrechden@wiley.law

Practice Areas

Cybersecurity
Government Contracts
National Security
Small Businesses
Strategic Competition & Supply Chain
Telecom, Media & Technology

- Broadening platform standards and interoperability by:

  1) Promoting open architecture so that components are interchangeable and DOD components can integrate new technologies across different systems;

  2) Adopting industry standards for aligning allies and partners to address capacity and capability gaps;

  3) Investing in research and development;

  4) Producing incentives and requirements for interoperability and exportability; and

  5) Exporting technologies to allies and partners during system design rather than post-production to reduce the costs throughout the procurement's life cycle.

- Utilizing the newly awarded Defense Industrial Base Consortium Other Transaction Agreement to "allow access to commercial solutions for defense requirements and innovations" through the use of other transactions for prototypes, research projects, and production.
- Strengthening the requirements process to curb cost overruns and gradual additions to capability requirements that change the scope of work – also known as "scope creep" – by supporting incremental development and advanced virtual modeling methodologies.
- Prioritizing COTS solutions where applicable to drive innovative and cost-effective supply options.
- Increasing DOD's access to intellectual property (IP) and data rights to enhance acquisition and sustainment by: (1) using modular open systems approaches; and (2) encouraging DOD activities to negotiate "specialized license agreements," to mitigate IP restrictions, as currently authorized in the DFARS.
- Expanding the use of multi-year procurement and non-FAR-based contract types as needed to lower costs of compliance and encourage other responsible offerors to compete.

Mitigating Cybersecurity Costs to Encourage Entry Into the Defense Industrial Ecosystem

DOD recognizes that the high costs of compliance for maintaining cybersecurity measures could disincentivize small businesses and suppliers from participating in government procurements. DOD suggests that these costs could instead be assumed by larger firms or otherwise mitigated. The 2023 DOD DIB Cybersecurity Strategy offers suggestions for improving current regulations, public-private partnerships, and interagency efforts geared toward enhancing industrial cybersecurity while reducing costs of compliance.

To further facilitate participation in the defense industrial ecosystem by small and medium-sized businesses, DOD intends to:

- Explore opportunities for expanding programs to mitigate costs of entry for small or mid-sized firms with innovative solutions for enhancing industrial capabilities;

- Promote investment in advanced manufacturing automation and regional manufacturing ecosystems; and
- Continue funding programs and offices such as the Defense Production Act loan and loan guarantee programs, Readiness and Environmental Protection Integration Program, Resilience Project Funding, and the Small Business Innovation Research and Small Business Technology Transfer programs – which invest more than $1 billion annually in small business technology.

Improving the Foreign Military Sales (FMS) Process

To address challenges with procuring and timely delivering military defense capabilities to allies during the Russian-Ukraine war and combat national security threats from China's rapid deployment of strategic military capabilities, DOD is ramping up the FMS program with the goal of increasing such sales.

DOD's acceleration of the FMS system aligns with its goals of:

- Aggressively expanding military production capacity that does not rely on foreign adversaries such as China and Russia;
- Generating new mechanisms for sharing technologies with allies;
- Strengthening relationships among allies and partners; and
- Improving planning for timely delivery of military capabilities to allies and partners.

Strengthening Prohibited Sources Policy and Increasing Supply Chain Visibility

According to the NDIS, DOD intends to work with Congress, other agencies, and global allies and partners to enhance supply chain visibility into cybersecurity systems and standard munitions items and eliminate industrial dependencies on foreign adversaries.

To further this effort, DOD intends to educate the industry on foreign threats, including defenses against cyberattacks. DOD encourages industry to use DOD's Project Spectrum, a free resource for information on cybersecurity and foreign ownership. Project Spectrum can be particularly useful for small businesses lacking the resources to implement their own programs for readiness, resiliency, and compliance.

***

Wiley's Government Contracts, Telecom, Media & Technology, and National Security practices closely track implementation of the NDIS and are prepared to update and help clients navigate any of the issues addressed by the recommendations and policy initiatives.