

**DENTONS**



# NDAA Update

Meagan Fackler  
Morgan Murphy

# Agenda

- Introduction
- FY 2024 NDAA
- FAR and DFAR Updates
- Cybersecurity Updates and Things to Come

# FY 2024 NDAA

# 2024 NDAA

## Topline Funding Levels

- FY24 Defense Funding Levels (in billions of dollars)
  - Department of Defense: \$841.4
  - Department of Energy: \$32.4
  - Defense-related Activities: \$0.4
  - NDAA Topline: \$874.2
  - Defense-related Activities Outside NDAA Jurisdiction: \$9.5
- National Defense Topline: \$883.7

# 2024 NDAA

## Artificial Intelligence

- Section 1521: Directs DoD to establish plans, strategies, and procedures in various areas relevant to AI. Authorizes the CDAO to obtain “access and control” of “any data” used by a DoD component.
- Section 1543: Establishes a prize competition open to defense contractors to develop technology that detects and watermarks the use of generative AI.
- Section 1544: Directs DoD to establish AI-related plans, strategies, and guidance, to include a requirement for plans to identify “commercially available and relevant” large language models, and “make such models available, as appropriate on classified networks.”

# 2024 NDAA

## Supply Chain Risks

- Section 805: Prohibits DoD from procuring goods, services, or technology from entities identified in an annual list published in the Federal Register as “Chinese military companies operating in the United States” or entities subject to their control.” This prohibition takes effect no later than June 2026, after being incorporated into the DFARS.
- Section 835: Requirement for domestic sourcing in the United States for manufactured articles, materials, and supplies connected with major defense acquisition programs.
- Section 804: Prohibits DoD from contracting with companies that maintain fossil fuel operations with the Russian government or the Russian energy sector.

# 2024 NDAA

## Supply Chain Risks (cont'd)

- Section 1513: Directs the Secretary of Defense, in coordination with the Director of the National Security Agency (“NSA”), to commence the conduct of a pilot program under which the Cybersecurity Collaboration Center of the NSA may collaborate with eligible persons for the purpose of evaluating the advisability of improving the cybersecurity of the semiconductor supply chain.
- Under the pilot program, parties will seek to improve the cybersecurity of the supply chain for the design, manufacturing, assembly, packaging, and testing of semiconductors.

# 2024 NDAA

## Technical Data Rights

- Section 808: Establishes a pilot program for the use of “innovative” intellectual property rights strategies to acquire technical data rights from contractors for certain programs to be identified by DoD as “necessary” for operation, maintenance, and installation purposes. Strategies used in a pilot program established under the section may include:
  - Use of an escrow account to verify and hold intellectual property data;
  - Use of royalties or licenses; or
  - Other strategies, as determined by the Secretary of Defense.



# 2024 NDAA

## Commercial Solutions Openings and Procurement Innovation

- Section 811: Instructs DoD to develop a streamlined process for developing its contract requirements with stated goals that include rapidly validating the ability for commercial products and services to meet DoD's needs.
- Section 813: Expands DoD's statutory authority to use Commercial Solutions Openings ("CSOs") – a competitive process for the acquisition of innovative commercial products and services – by requiring that DoD exercise its CSO authority at least four times per fiscal year.

# 2024 NDAA

## Other Provisions

- Section 318: Prohibits DoD, for one year, from requiring that defense contractors disclose greenhouse gas (“GHG”) inventory or emissions as a condition of receiving a defense contract, absent a waiver.
  - The FAR Council issued a proposed rule requiring contractors to disclose GHG emissions and climate-related risk and set targets to reduce their GHG emissions. The NDAA provision effectively bars DoD from making such GHG representations a condition of a contract award.
- Section 820: Permits DoD to enter into multiyear contracts for the purchase of property to promote industrial base security.
- Section 864: Prohibits Companies claiming status as Service-Disabled Veteran-Owned Small Businesses (“SDVOSBs”) from relying on self-certifications, and requires certification by the Small Business Administration (“SBA”).

# 2024 NDAA

## Other Provisions

- Section 831: Establishes emergency acquisition authority for purposes of replenishing United States stockpiles of defense articles.
- Section 123: Authorizes the Navy to enter into multiyear procurement contracts for up to thirteen Virginia class submarines.
- Section 1414: Directs DoD to expand secure sources of supply of critical minerals, including rare earth elements, in the United States, and in countries that are allies and partners of the United States to meet defense sector needs for such materials.

# 2024 NDAA

## Other Provisions

- Section 801: Commercial Nature Determination Memo Available to Contractor
  - Contractors can now get commercial item determinations
- Section 802: Modification of Truthful Cost or Pricing Data Submissions & Report
  - Increased pressure on contractors to provide uncertified cost or pricing data.
- Section 809: Pilot Program for Anything-as-a-Service
  - Requires establishment of pilot program to explore the use of “anything-as-a-service” delivery models to address defense needs.
  - “Anything-as-a-service” is technology supported capabilities (which could include software, hardware, or equipment data, and labor or services) that are customizable, scalable, and billed based on actual usage (e.g. subscription models like software as a service (SaaS), platform as a service (Paas), and infrastructure as a service (IaaS)).

# 2024 NDAA

## Other Provisions

- Section 862: Payment of Subcontractors
  - Strengthens remedies against prime contractors who fail to timely pay their small business subcontractors
- Section 865: Consideration of the Past Performance of Affiliate Companies of Small Businesses
  - For DoD contracts, past performance of affiliates will be considered as past performance of the small business bidder if relevant
- Section 5101: Prohibition of Demand for Bribe
  - Criminal offense for foreign officials to request/receive/agree to receive a bribe.

# FAR and DFARS Updates

# FAR Updates

- Use of Project Labor Agreements for Federal Construction Projects
  - Dec. 22, 2023, final rule requiring use of PLAs for large-scale (\$35 million or more) construction projects, unless an exception applies
- Improving Consistency for Procedures on Suspension and Debarment
  - Jan. 9, 2024, propose to amend FAR to improve the consistency between procurement and nonprocurement procedures on suspension and debarment.
  - Goal: to modify FAR to be closer aligned with the suspension and debarment procedures in the Nonprocurement Common Rule (“NCR”): revised definitions and add 7 aggravating or mitigating factors that suspending and debarring officials should consider before making a decision.
- Pay Equity and Transparency in Federal Contracting
  - Jan. 30, 2023, propose to prohibit contractors and subs from asking for information about applicants’ compensation history when making employment decisions.
  - Applies to recruitment and hiring for any position to perform work in connection with any contract, and applicants are to be provided with notice.
  - Must disclose compensation in job advertisements.

# DFARS Updates

- Inapplicability of Additional Defense-Unique Laws and Certain Non-Statutory DFARS Clauses to Commercial Item Contracts
  - Nov. 17, 2023, proposing to review the DFARS and propose revisions to eliminate certain contract clause requirements applicable to COTS item subcontracts as well as commercial product and service acquisitions.
- Cybersecurity Maturity Model Certification (“CMMC”) Program
  - Dec. 26, 2023, proposes to establish requirements for a comprehensive and scalable assessment mechanism to ensure defense contractors and subcontractors implement required security measures to expand application of existing security requirements for Federal Contract Information (“FCI”) and add new Controlled Unclassified Information (“CUI”) security requirements for certain priority programs.
  - The CMMC Program provides the DoD a mechanism to verify that a defense contractor or subcontractor has implemented the security requirements at each CMMC Level and is maintaining that status across the contract period of performance



# Cybersecurity Updates

# Increased Government Focus

## Background

- Throughout 2023, new proposed rules, guidance, and executive orders showing an increased focus on cybersecurity protections.
- This correlates with continued rise in cyber threats and data breaches.

Data breach affects 57,000 Bank of America accounts

The Pentagon is notifying individuals affected by 2023 email data breach

Data of half the population of France stolen in its largest ever cyberattack. This is what we know

# Pending Proposed Rules

- In line with EO 14028, “Improving the Nation’s Cybersecurity,” there are many pending proposed rules focused on cybersecurity.
- Proposed rules cover:
  - New requirements to increase sharing of information with government about cyber threats and incident reporting and response obligations (Case No. 2021-017)
    - Quick cyber incident reporting (within 8 hours)
    - New FAR clauses: 52.239-AA, Security Incident Reporting Representation; 52.239-ZZ, Incident and Threat Reporting and Incident Response Requirements for Products or Services Containing ICT
  - Standardizing cyber requirements for unclassified federal information systems (Case No. 2021-019)
    - FAR 52.239-XX, Federal Information Systems Using Cloud Computing Services
    - FAR 52.239-YY, Federal Information Systems Using Non-Cloud Computing Services
  - New FAR Part 40 being created for cybersecurity supply chain requirements
    - Final rule to be published soon

# Pending Proposed Rules

- Software self-attestation requirement:
  - EO 14028 and OMB memoranda
  - Agencies will be required to obtain self-attestation from software producer before using any software that “affects” government information or will be used on government information systems
  - For critical software, 3 months after OMB approves the self attestation form (expected soon), and 6 months for all other software
- FASCA/SECURE Technology Act
  - FAR 52.204-28, Federal Acquisition Supply Chain Security Act Orders – Federal Supply Schedules, Governmentwide Acquisition Contracts, and Multi-Agency Contracts (Dec. 2023)
  - FAR 52.204-29, Federal Acquisition Supply Chain Security Act Orders – Representation and Disclosures (Dec 2023)
  - FAR 52.204-30, Federal Acquisition Supply Chain Security Act Orders – Prohibition (Dec 2023)