

A Standardized Pathway to Cybersecurity Compliance for the Defense Industrial Base

The NCODE Pilot: Accelerating DFARS Adoption for Small Businesses

Why You Are Receiving This White Paper

As a small business supporting Golden Dome for America (GDA), your organization has been identified as a potential participant in the Next-Generation Commercial Operations in Defended Enclaves (NCODE) pilot program.

The NCODE pilot is designed to help eligible small businesses simplify their path toward Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012, safeguarding covered defense information, compliance by connecting them with government-contracted, vetted External Service Providers (ESPs) to protect Controlled Unclassified Information (CUI).

Over the coming weeks, **you may be contacted by ATX Defense or Exostar regarding cloud enclave services** available to your business, at no initial cost to you, through the NCODE pilot. This document provides an overview of the program, explains the purpose of the pilot, and outlines what you can expect throughout the process.

Executive Summary

The U.S. Department of War (DoW) has identified cybersecurity as a top priority to protect sensitive information and enhance the security of the Defense Industrial Base (DIB). The Cybersecurity Maturity Model Certification (CMMC) program was incorporated into the DFARS 252.204-2021 effective 10 November 2025, via 48 CFR § 204 and is a key component of this initiative, creating a unified standard for the implementation of cybersecurity measures. CMMC is currently in Phase 1 implementation which requires self-attestation of compliance with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 “Protecting Controlled Unclassified Information (CUI) in Nonfederal Systems and Organizations”. However, many small businesses within the DIB face significant challenges in meeting these rigorous requirements due to cost, complexity, and a lack of in-house expertise.

To address this, the U.S. Army and the GDA program have funded the NCODE pilot program. NCODE is designed to create a standardized, cost-effective pathway for small businesses to achieve NIST SP 800-171 compliance. It does so by establishing a marketplace of vetted External Service Providers (ESPs) that offer pre-configured, compliant solutions.

This white paper explains the purpose of the NCODE pilot, how it supports small businesses in achieving cybersecurity compliance, the role of government-approved External Service Providers (ESPs), and what participating organizations can expect as the pilot progresses.



Figure 1. NCODE pilot process

1. Introduction: The Cybersecurity Imperative

In an era of persistent cyber threats, safeguarding the defense supply chain is a matter of national security. The DoW handles a vast amount of sensitive data, including Federal Contract Information (FCI) and CUI which require safeguarding and dissemination controls. The protection of this information is paramount. To that end, the DoW commissioned the CMMC program to assess and enhance the cybersecurity posture of contractors who serve the DoW.

The CMMC program standardizes a contractor's compliance with existing information safeguarding requirements and institutionalizes the adoption of security best practices. While essential, the path to CMMC compliance can be a daunting and resource-intensive endeavor, particularly for the small businesses that form the backbone of the DIB.

2. The Solution: The NCODE Pilot Program

The NCODE program is a forward-thinking initiative designed to directly address these challenges. Funded primarily by the U.S. Army and the GDA program, NCODE is building a

marketplace of verified ESPs to offer small businesses a standardized and streamlined pathway to DFARS 252.204-2012 and 252.204-2021 compliance.

The marketplace will transition to the Cyber Engagement Forum (Cyber EF) after the pilot. The mission of the Cyber EF is to support and promote the attainment of cybersecurity conformity through continuous engagement with industry and government in areas of training, education, outreach, and market facilitation.

The core mission of NCODE is to:

- **Democratize Cybersecurity:** Make NIST SP 800-171 compliance accessible and affordable for businesses of all sizes.
- **Reduce Complexity:** Offer pre-vetted, "out-of-the-box" solutions that meet NIST SP 800-171 requirements at various levels.
- **Accelerate Adoption:** Provide a clear, repeatable, and efficient process for achieving and maintaining compliance.

3. How the NCODE Pilot Works

The NCODE pilot provides a standardized pathway for eligible small businesses to work toward DFARS 252.204-2012 and 252.204-2021 cybersecurity compliance through trusted, government-contracted ESPs.

The process is designed to simplify compliance by reducing technical complexity and providing pre-vetted solutions.

The pilot follows a straightforward process:

1. Eligible small businesses are identified for participation.
2. Organizations may be contacted by a government-approved External Service Provider (currently ATX Defense or Exostar).
3. The ESP works with the organization to determine the most appropriate cybersecurity solution.
4. The ESP and SB, through a Shared Responsibility Matrix (SRM), implements the recommended compliant environment and services.
5. The organization is better positioned to meet applicable DFARS cybersecurity requirements.

This standardized approach reduces administrative burden while helping organizations improve their cybersecurity posture.

4. The NCODE Marketplace and ESPs

The NCODE Marketplace serves as the central hub connecting eligible small businesses with trusted, government-contracted External Service Providers (ESPs). These providers offer standardized cybersecurity solutions designed to simplify compliance while reducing the cost and complexity traditionally associated with meeting DFARS cybersecurity requirements. The U.S. Army Contracting Command (ACC) has contracted with **ATX Defense** and **Exostar** as the first two of up to eight ESPs to pioneer this marketplace.

These ESPs offer a suite of services for **Productivity** tools (i.e. Google Workspace, Microsoft 365). In the future, the NCODE Marketplace will host ESPs that offer **DevSecOps (DSO)**, **Model-Based Systems Engineering (MBSE)**, and **Manufacturing** environments. By leveraging the NCODE marketplace, small businesses can select a verified ESP that provides a compliant enclave for their operations, significantly reducing the burden and cost of building a secure environment from scratch.

Current ESPs:

At the launch of the NCODE pilot, the U.S. Army Contracting Command (ACC) has contracted with the following ESPs:

Provider	Status
ATX Defense	Current pilot provider
Exostar	Current pilot provider

These providers will engage directly with participating organizations to discuss available services, answer questions, and support implementation activities throughout the pilot.

As the program matures, additional vetted providers will be incorporated into the NCODE Marketplace.

5. Advocacy and Funding: A Public-Private Partnership

The success of the NCODE pilot is driven by the strong advocacy and financial commitment of its founding partners:

- **The U.S. Army:** As a primary stakeholder in a secure DIB, the U.S. Army has provided critical funding and contractual mechanisms to launch the NCODE pilot, demonstrating its commitment to strengthening its supply chain.
- **The Golden Dome for America (GDA):** The GDA's involvement underscores the importance of public-private partnerships in tackling national security challenges.

Its advocacy and funding help bridge the gap between government requirements and industry capabilities.

This collaboration ensures that NCODE is aligned with both military needs and the realities of the commercial marketplace.

6. Conclusion and Next Steps

The NCODE pilot represents a significant step toward making protection of government CUI more accessible for small businesses supporting the Defense Industrial Base.

By leveraging trusted External Service Providers, the pilot reduces the complexity, cost, and administrative burden traditionally associated with cybersecurity compliance while strengthening the resilience of the Defense Industrial Base.

What to Expect Next

If your organization has been identified for participation in the NCODE pilot:

- You may be contacted by ATX Defense or Exostar regarding available services.
- Participation details and available offerings will be explained during provider outreach.
- Additional guidance and information will be shared as the pilot continues to expand.

Frequently Asked Questions

Who is eligible for the NCODE pilot?

Organizations identified by the U.S. Army as potential participants supporting the Defense Industrial Base (DIB).

Is participation mandatory?

No. Participation is voluntary. Organizations will receive additional information during provider outreach before making any decisions.

Will participation require an assessment against NIST SP 800-171 requirements?

The NCODE pilot is designed to simplify the path toward cybersecurity compliance by leveraging trusted External Service Providers. At this time, the CMMC guidance calls for self-attestation in the Supplier Performance Risk System (SPRS) only.

Who will contact my organization?

Participating organizations may be contacted by an ESP, a government-contracted service provider supporting the pilot.

What happens after I am contacted?

The provider will explain available services, discuss your organization's needs, and outline potential next steps.