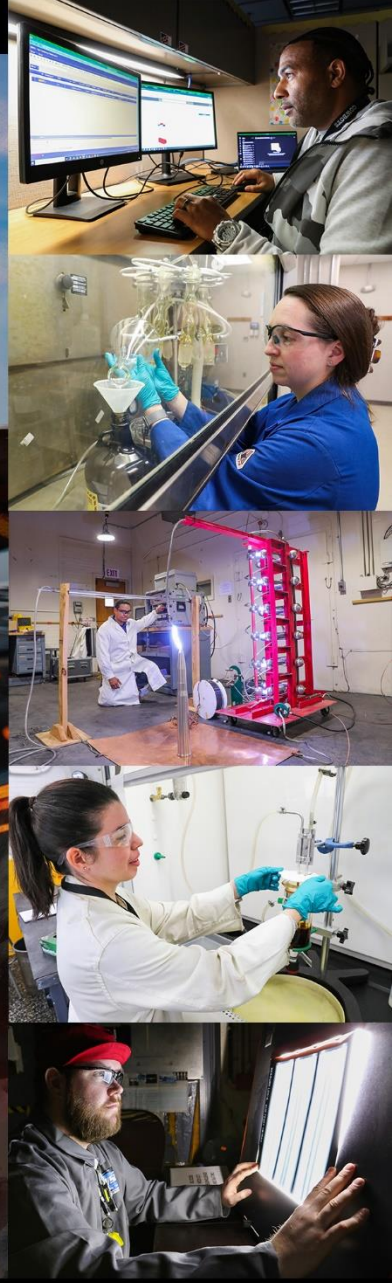
NAVSEA
NAVAL SEA SYSTEMS COMMAND

NAVAL SURFACE WARFARE CENTER
INDIAN HEAD DIVISION

26 August 2026

Cybersecurity Maturity Model Certification (CMMC) Virtual Industry Day



NAVSEA
NAVAL SEA SYSTEMS COMMAND

NAVAL SURFACE WARFARE CENTER
INDIAN HEAD DIVISION

AGENDA

- Welcome
- Who we are
- What we do
- Small Business Information
- CMMC Presentation
- *Move America*
- *U.S. Army's Next-Generation Commercial Operations in Defended Enclaves (NCODE) Team*
- *Break*
- *Department/Division Briefs*
- *Closing Remarks*

NAVSEA
NAVAL SEA SYSTEMS COMMAND

NAVAL SURFACE WARFARE CENTER
INDIAN HEAD DIVISION

Who We Are

- As a field activity of the Naval Sea Systems Command, and part of the Navy's Science and Engineering Establishment, NSWC IHD is the Navy's premier facility for ordnance, energetics and explosive ordnance disposal (EOD) solutions. We support the warfighter of today and tomorrow through discoveries that anticipate the next generation's future needs.

- NSWC IHD- As the Department of War's (DoW) largest full-spectrum energetics facility and the Navy's energetic enterprise leader, NSWC IHD employs a primarily Maryland-based workforce of nearly 2,700. NSWC IHD also has two official detachments and six off-site locations, including sites in Picatinny, New Jersey; McAlester, Oklahoma; Rock Island, Illinois; and Ogden, Utah; and employees stationed throughout the world.

- The command's capabilities address all aspects of the energetics technical discipline including: basic research, applied technology, technology demonstration and prototyping, engineering development, acquisition, low-rate production, in-service engineering/mishaps, failure investigations, surveillance, EOD technology/information and demilitarization. When the military experiences problems with current weapon systems or encounters new threats on the battlefield, NSWC IHD answers the call to provide the solution.

NAVSEA
NAVAL SEA SYSTEMS COMMAND

NAVAL SURFACE WARFARE CENTER
INDIAN HEAD DIVISION

What We Do

- NSWC IHD is the nation's only design and development agent for underwater warheads and explosives.
- NSWC IHD is designated as the Navy's Manufacturing Technology Center for Energetics, one of seven Centers of Excellence established by the Office of Naval Research's ManTech Program.
- NSWC IHD's explosive modeling experts developed high-fidelity underwater hydrocodes with German researchers, providing the Navy a capability to predict underwater explosive performance and affect for various lethality and vulnerability applications. Extensions of the Dynamic System Mechanics Advanced Simulation are used to help improve future ship hull designs.
- NSWC IHD provides **real-time** technical support to EOD responders and specializes in developing and delivering technology, knowledge, tools, equipment, training and life-cycle support for the joint services.

Jennifer Barnidge

Deputy Director for Small Business (NSWC IHD) and SSBO (Acting), PAE MUNITIONS

NAVSEA
NAVAL SEA SYSTEMS COMMAND

NAVAL SURFACE WARFARE CENTER
INDIAN HEAD DIVISION

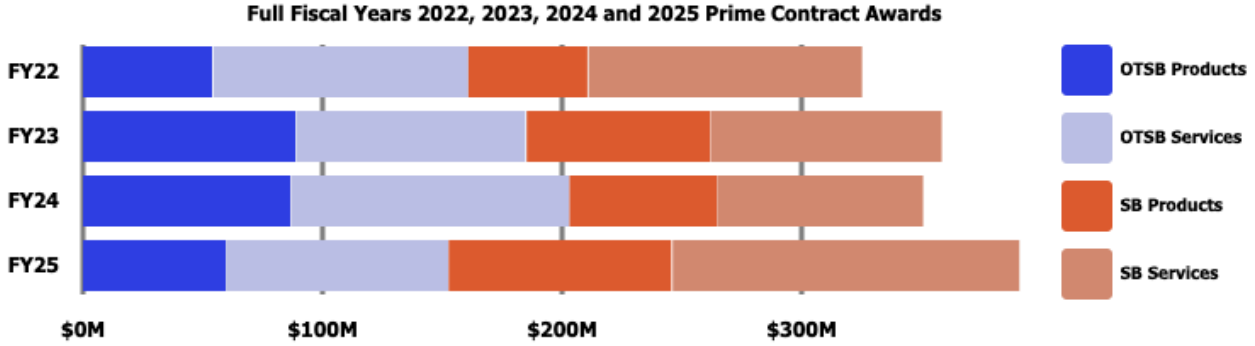
Small Business Metrics

NSWC INDIAN HEAD (UIC: N00174)

Validated Fiscal Year 2025 FPDS-NG/SAM.gov Data [Data extracted on 06 March 2026]

Total: $391.14M

$152.68M	$238.77M
Other Than SB	Small Business



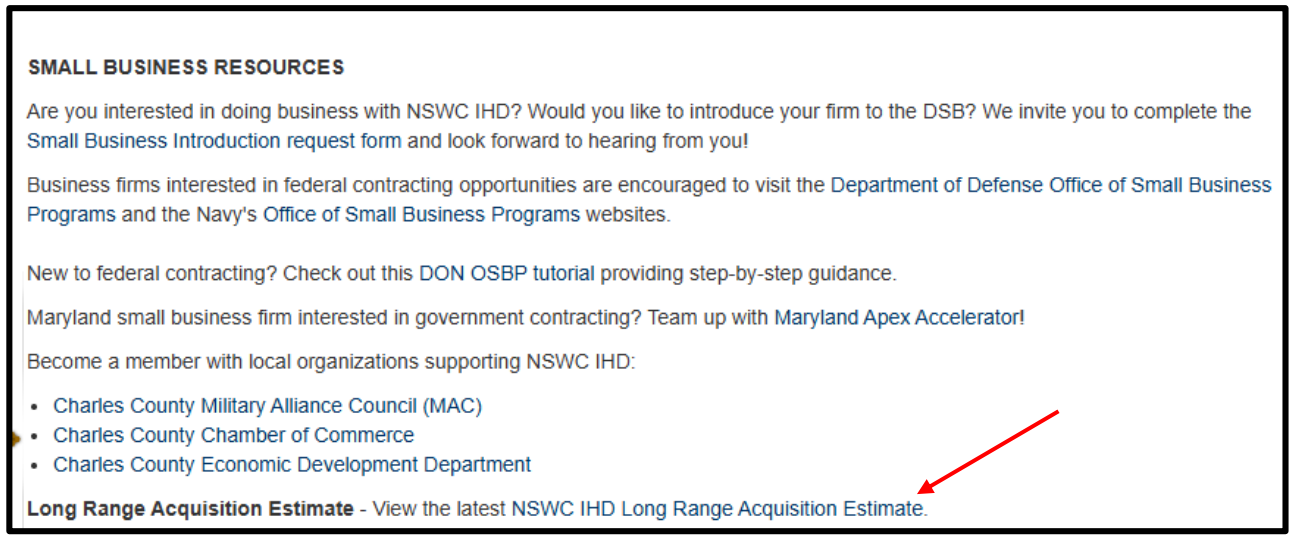
$238,766,864	$86,409,107	$1,574,675	$18,041,822	$10,931,168
Small Business	Small Disadvantaged	Service-Disabled	Women Owned	HUBZone

NAVSEA NAVAL SEA SYSTEMS COMMAND | NAVAL SURFACE WARFARE CENTER INDIAN HEAD DIVISION

Doing Business with NSWC Indian Head

- Review NSWC Indian Head's advanced planning tool, Long-Range Acquisition Estimate (LRAE), to preview upcoming procurement and contract opportunities. NSWC Indian Head's LRAE will be updated by the end of the calendar year.

- Visit the site at: https://www.navsea.navy.mil/Home/Warfare-Centers/NSWC-Indian-Head/Partnerships/Small-Business/



SMALL BUSINESS RESOURCES

Are you interested in doing business with NSWC IHD? Would you like to introduce your firm to the DSB? We invite you to complete the Small Business Introduction request form and look forward to hearing from you!

Business firms interested in federal contracting opportunities are encouraged to visit the Department of Defense Office of Small Business Programs and the Navy's Office of Small Business Programs websites.

New to federal contracting? Check out this DON OSBP tutorial providing step-by-step guidance.

Maryland small business firm interested in government contracting? Team up with Maryland Apex Accelerator!

Become a member with local organizations supporting NSWC IHD:

- Charles County Military Alliance Council (MAC)
- Charles County Chamber of Commerce
- Charles County Economic Development Department

Long Range Acquisition Estimate - View the latest NSWC IHD Long Range Acquisition Estimate.

Note: The slides from today's CMMC Virtual Industry Day will be posted to the same link.

Cybersecurity Maturity Model Certification (CMMC)

Ashleigh Bowie
Contracting Officer, NSWC IHD

NAVSEA
NAVAL SEA SYSTEMS COMMAND

NAVAL SURFACE WARFARE CENTER
INDIAN HEAD DIVISION

What? Why? When?

The Cybersecurity Maturity Model Certification (CMMC) is a Department of War (DoW) program designed to standardize and enforce robust cybersecurity practices across the Defense Industrial Base (DIB), ensuring the rigorous protection of Federal Contract Information (FCI) and Controlled Unclassified Information (CUI):

- **Federal Contract Information (FCI)**: As defined in section 4.1901 of the Federal Acquisition Regulation (FAR), FCI is "information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, excluding information provided by the Government to the public (such as that on public websites) or simple transactional information, such as that necessary to process payments."

- **Controlled Unclassified Information (CUI)**: As outlined in Title 32 CFR 2002.4(h), CUI is "information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls." For more information regarding specific CUI categories and subcategories, see the DoW CUI Registry website.

The program aligns with FAR RFO 52.240-93 as well as the NIST SP-800-171 requirements.

CMMC applies to all solicitations and contracts issued after 10 November 2025, in which a defense contractor or subcontractor will process, store, or transmit FCI or CUI on its unclassified contractor information systems, with the following **exceptions:**

- Actions below the micro-purchase threshold ($10,000 or less)
- Commercial Off-the-Shelf (COTS) {not to be confused w/ commercial services…}

Implementation is being conducted via a **phased approach.** We are currently in Phase 1. As of 13 July 2026, it is unknown if/when we will transition into the remaining phases.

NAVSEA
NAVAL SEA SYSTEMS COMMAND

NAVAL SURFACE WARFARE CENTER
INDIAN HEAD DIVISION

What? Why? When?

- On July 13, 2026, the Department of War announced the immediate suspension of the Cybersecurity Maturity Model Certification (CMMC) Phase II requirements, which was originally scheduled for November 10, 2026. All Phase I self-assessment requirements remain firmly in place. The DoW has begin a comprehensive review of CMMC aimed at aligning with the Secretary of War Pete Hegseth's Acquisition Transformation System (ATS) directives prioritizing speed to capability, lowering barriers for small, medium, and non-traditional businesses, and replacing bureaucratic compliance with scalable, resilient cybersecurity measures.

- **During this interim period, the DoW will enforce cybersecurity compliance with the NIST SP 800-171 Rev 2 standard through self-assessments.**

- It is critical to note that this action does not eliminate the requirement for companies to protect federal data. All defense contractors and subcontractors remain contractually obligated to safeguard covered defense information in accordance with DFARS clause 252.204-7012.

NAVSEA
NAVAL SEA SYSTEMS COMMAND

NAVAL SURFACE WARFARE CENTER
INDIAN HEAD DIVISION

What is the difference between Level 1 and Level 2?

Level 1 (self) focuses on the protection of FCI and is aligned with 15 minimum security controls identified in FAR RFO 52.240-93, considered to be "basic cyber hygiene". Examples include:

- Limiting information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).
- Controlling information posted or processed on publicly accessible information systems.
- Authenticating (or verifying) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.
- Sanitizing or destroying information system media containing FCI before disposal or release for reuse.

Level 2 (self) focuses on the protection of FCI (see Level 1), but also incorporates the 110 security requirements specified in NIST SP 800-171 Rev. 2, categorized by the following 14 domains:

- Access Control – 22 requirements
- Awareness & Training – 3 requirements
- Audit & Accountability – 9 requirements
- Configuration Management – 9 requirements
- Identification & Authentication – 11 requirements
- Incident Response – 3 requirements
- Maintenance (MA) – 6 requirements
- Media Protection (MP) – 9 requirements
- Personnel Security (PS) – 2 requirements
- Physical Protection (PE) – 6 requirements
- Risk Assessment (RA) – 3 requirements
- Security Assessment (CA) – 4 requirements
- System and Communications Protection (SC) – 16 requirements
- System and Information Integrity (SI) – 7 requirements

NAVSEA
NAVAL SEA SYSTEMS COMMAND

NAVAL SURFACE WARFARE CENTER
INDIAN HEAD DIVISION

What clauses are required?

➢ **DFARS 252.204-7025 - Notice of Cybersecurity Maturity Model Certification Level**

Its primary purpose is to put bidders on notice:

- It is inserted into a Request for Proposal (RFP) or solicitation to explicitly tell you what CMMC level you must have to be eligible to win the contract
- When a contracting officer inserts this provision into an RFP, they must fill in the blanks to specify:
  - The exact CMMC Level required (Level 1, Level 2, or Level 3)
  - The assessment type required (e.g., self-assessment vs. a C3PAO third-party audit)
  - Verification timeline (confirming that your certification must be active and verified in the DoW's Supplier Performance Risk System (SPRS) at the time of award)

➢ **FAR 52.240-93- Basic Safeguarding of Covered Contractor Information Systems**

Formerly known as FAR 52.204-21, this clause is the standard entry-level cybersecurity requirement for any government contractor.

- It protects Federal Contract Information (FCI) (basic contract details, emails, schedules, billing).
- It mandates the implementation of 15 basic security controls (which map directly to CMMC Level 1). These controls cover fundamental cyber hygiene, including:
  - Using firewalls and antivirus software.
  - Restricting system access to authorized users only.
  - Requiring unique user logins and passwords.
  - Escorting visitors and physically securing office spaces.
- Self-assessment. No third-party audits are required under this clause alone.
- Prime contractors must flow this clause down to all subcontracts where the subcontractor will handle, store, or transmit FCI.

NAVSEA
NAVAL SEA SYSTEMS COMMAND

NAVAL SURFACE WARFARE CENTER
INDIAN HEAD DIVISION

What clauses are required?

➢ **DFARS 252.204-7021: Cybersecurity Maturity Model Certification (CMMC) Requirements**
This is the "master" DoD clause that legally binds CMMC certification to the contract award process.

- It protects both FCI and Controlled Unclassified Information (CUI) (highly sensitive technical designs, military schematics, and operations data).
- It mandates that the contractor must possess a specific CMMC certification level (Level 1, 2, or 3) determined by the DoD to be appropriate for the sensitivity of the contract's information.
- You must have the required CMMC certification at the time of contract award and maintain it for the entire duration of the contract. If your certification expires or is revoked, you can lose the contract.
- Varies by level. Level 1 requires an annual self-assessment, while Level 2 and Level 3 require formal, independent audits by accredited third-party assessors (C3PAOs) or government assessors (DIBCAC) every three years.
- Prime contractors must flow this down to subcontractors at all tiers. The level flowed down must match the type of data the subcontractor will handle (e.g., if a subcontractor only handles FCI, they only need Level 1; if they handle CUI, they must have Level 2).

If you see DFARS 252.204-7025 in a solicitation, it is your cue to immediately check your system's current CMMC certification status!!

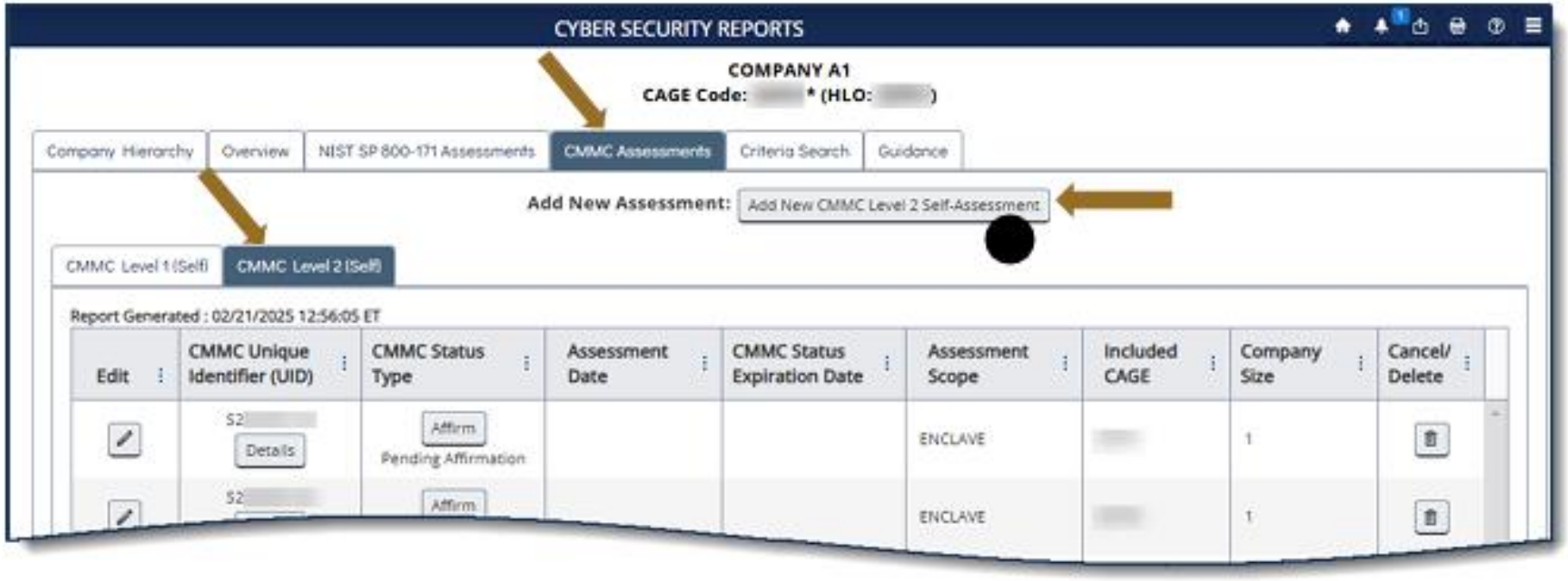
NAVSEA
NAVAL SEA SYSTEMS COMMAND

NAVAL SURFACE WARFARE CENTER
INDIAN HEAD DIVISION

How to achieve compliance?

- The process for certifying CMMC compliance involves utilizing Supplier Performance Risk System (SPRS) within the Procurement Integrity Enterprise Environment (PIEE) module. https://www.sprs.csd.disa.mil/pdf/CMMCL2SelfQuickEntryGuide.pdf

3.1 Add New CMMC Level 2 Self-Assessment: Within the CMMC Assessments and CMMC Level 2 (Self) tabs, select "Add New Level 2 CMMC Self-Assessment".

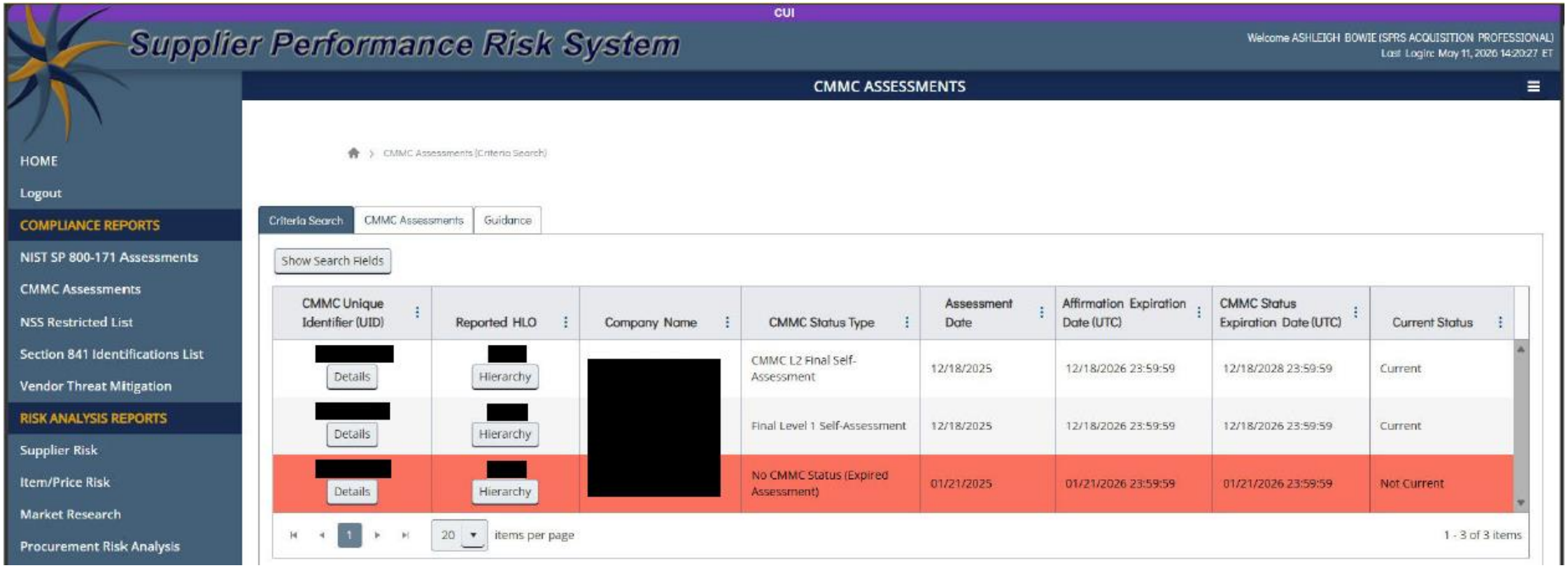


NAVSEA
NAVAL SEA SYSTEMS COMMAND

NAVAL SURFACE WARFARE CENTER
INDIAN HEAD DIVISION

How is the government verifying compliance?

Contracting officers (COs) must verify the contractor's CMMC status in SPRS before signing any contract, task order, or modification:



NAVSEA
NAVAL SEA SYSTEMS COMMAND

NAVAL SURFACE WARFARE CENTER
INDIAN HEAD DIVISION

What is the cost?

Total compliance expenses hinge on your required CMMC tier, network complexity, current security baseline, and market demand for IT services.

- Level 1 (Foundational): Est. 60–90 Days. This level focuses on validating existing basic cyber hygiene. If your organization already complies with FAR requirements, costs remain minimal.

- Level 2 (Advanced): Est. 6–9 Months. This level requires substantial investment. It mandates an independent Certified Third-Party Accessor Organization (C3PAO) audit and typically drives significant hardware, software, and outsourced IT upgrades.

Phase no.	Cost component	Description	Estimated yearly expense	Frequency
1.	Readiness	Assessment, CUI Scoping	00 – 0	One-time (Initial)
2.	Remediation		,000 – $150,000+	One-time (Initial)
3.	C3PAO audit fee		$35,000 – ,000	Triennial
4.	Maintenance & recertification	criptions, internal itoring, training, and ongoing compliance activities	00 – ,000	Annual (Recurring)
Total estimated year 1 expenditure (Phases 1–3 + Phase 4 Annual)			**$70,000 – $250,000+**	—

Source: https://www.scrut.io/hub/cmmc/certification-cost

NAVSEA
NAVAL SEA SYSTEMS COMMAND

NAVAL SURFACE WARFARE CENTER
INDIAN HEAD DIVISION

What if my company is non-compliant?

Contracting officers are prohibited from proceeding with an award/period of performance (POP) extension if the required CMMC level is not met. In the case of existing awards, if the CMMC level is not met, contracting officers may exercise their "standard contract remedies" and the company may be ineligible for additional awards that require CMMC.

DFARS (RFO) 240.371-4 Procedures.

(a) CMMC level. The contracting officer must include the CMMC level (see 32 CFR 170.19) required by the program office or requiring activity in the solicitation provision and contract clause prescribed at 240.371-5.

(b) Award. Contracting officers **must check SPRS and not award** a contract, task order, or delivery order to an offeror that does not have a current CMMC status posted in SPRS at the CMMC level (see 32 CFR 170.15 through 170.18) required by the solicitation, or higher, for each CMMC Unique Identifier (UID) provided by the offeror. The CMMC UIDs are applicable to each of the contractor information systems that will process, store, or transmit FCI or CUI and that will be used in performance of the contract.

(c) Option exercise or period of performance extension. Contracting officers **must check SPRS and not exercise an option or extend the period of performance** on a contract, task order, or delivery order, unless the contractor has a current CMMC status posted in SPRS at the CMMC level (see 32 CFR 170.15 through 170.18) required by the contract, task order, or delivery order, or higher, for each CMMC UID provided by the contractor. The contractor's CMMC UIDs are applicable to each of the contractor information systems that process, store, or transmit FCI or CUI and that are or will be used in performance of the contract.

NAVSEA
NAVAL SEA SYSTEMS COMMAND

NAVAL SURFACE WARFARE CENTER
INDIAN HEAD DIVISION

DoW – Request for Information

Alongside the pause, the DoW published an official Request for Information (RFI) on SAM.gov titled "Reforming CMMC and Reducing Compliance Burden for the Defense Industrial Base (DIB)"

- **The RFI specifically asked contractors to detail their compliance challenges, resource constraints, and the overall financial burden of CMMC**
- **Five out of seven questions in the RFI focused entirely on finding ways to reduce costs and complexity for small and non-traditional businesses**
- **Public comments and written feedback were accepted up until 12:00 PM ET on Friday, August 14, 2026**

NAVSEA
NAVAL SEA SYSTEMS COMMAND

NAVAL SURFACE WARFARE CENTER
INDIAN HEAD DIVISION

WHY CMMC IS CRITICAL FOR NSWC IHD

The Warfighting Impact

- NSWC IHD develops, scales, and produces the critical energetics and ordnance that power the fleet.
- Compromised technical data, manufacturing processes, or material specifications gives adversaries an asymmetric advantage and directly threatens warfighter safety.

Our Industry Partners

- Our industry partners are a direct extension of our command. You manufacture our hardware, construct our facilities, and provide mission-critical services.
- Because our supply chain is deeply integrated, your network security is our national security.

Protecting the Technical Baseline

- Whether you are handling technical data packages (TDPs) for warheads, blueprints for critical infrastructure, or operational logistics data, this Controlled Unclassified Information (CUI) must be locked down.
- CMMC ensures that every tier of our partnership maintains a hardened cybersecurity posture.

CMMC is not a compliance checklist it is how we secure our warfighter.

NAVSEA
NAVAL SEA SYSTEMS COMMAND

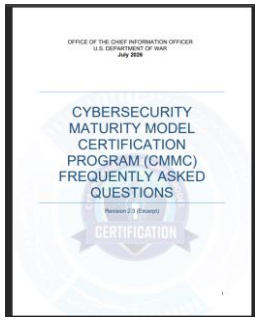
NAVAL SURFACE WARFARE CENTER
INDIAN HEAD DIVISION

CMMC Resources

- The DoW CIO website on the topic has several resources available to industry, such as:

- The CMMC Accreditation Body, currently the Cyber AB, has a marketplace of certified CMMC assessors, professionals, and registered practitioner organizations that companies can engage now to prepare for CMMC implementation: https://cyberab.org/marketplace
- The Warfighting Acquisition University offers free online cybersecurity training, including convenient micro-learning articles and videos about CMMC topics.
  - Visit https://www.waru.edu/cybersecurity/cyber-solutions to access free training on various cybersecurity topics, including courses on CMMC available under the 'CMMC Resources from the DoW CIO' drop-down menu.
  - Visit https://www.waru.edu/acquipedia?combine=cmmc&title=&field_functional_area_target_id=All&field_topic_area_target_id=All to access free CMMC micro-learning videos on a variety of CMMC topics.
- The Department of War-Defense Industrial Base Collaborative Information Sharing Environment website has a list of no-cost cybersecurity resources to reduce barriers to defense industrial base community compliance and support contract cybersecurity efforts at https://www.dc3.mil/Missions/DIB-Cybersecurity/DIB-Cybersecurity-DCISE/ under "Policy, Standards, and Resources" then "DoD DIB Cybersecurity Capabilities and Support."
- The Department of War Office of Small Business Programs has compiled a list of resources on their website aimed at helping small- and medium-sized businesses understand security requirements and reach compliance: https://business.defense.gov/Resources/FAQs/

Source: https://dodcio.defense.gov/Portals/0/Documents/CMMC/FAQsv6.pdf



Move America
Duane Wilson

NSWC IHD VIRTUAL INDUSTRY DAY

CMMC - Plan of Action

Evidence over Narrative

Practical approaches to CMMC after the pause — scoping, reciprocity, and what six companies learned.

Duane Wilson · Move America · Hanover, MD

JULY 13, 2026

What Changed — and What Did Not

Suspended

- Phase 2 third-party assessment (was set for Nov 10, 2026)
- Level 2 (C3PAO) and Level 3 designations during the review
- Existing clauses exit by modification — at the next option period, not today
- No waivers available during suspension

Still in Force

- DFARS 252.204-7012 and FAR 52.204-21
- NIST SP 800-171 Rev 2 — not Rev 3
- Level 1 and Level 2 self-assessment, posted in SPRS
- Annual senior-official affirmation — with False Claims Act weight
- Government-led assessments

The reform RFI closed August 14. Task Force recommendations are expected mid-September; the earliest realistic formal action is mid-October.

> The assessor didn't disappear. The assessor became you.

THE PATTERN

Documentation Outran Verification

Every organization writes the document first, because the document is what gets asked for. The configuration is supposed to catch up.

Narrative
Policies and procedures that describe intent.

Approval
Sign-off on the written security posture.

Requirement
Documented controls and requested behaviors.

Configuration
Actual systems and settings that must align.

Our Own Audit

- A complete, FedRAMP-grade SSP — 300+ documented controls, policies, procedures, diagrams
- Then we ran checks against our own boundary
- Six findings where document and configuration disagreed — all closed
- Nobody lied. Not one was dishonesty.

Six Companies, One Year

- Taken from zero to assessment-ready alongside Maryland APEX
- All six finished with documentation substantially complete
- All six had the same critical path remaining: **evidence**
- The hard part was never understanding the requirements

⚠ With an assessor, that gap gets caught expensively. Without one, it gets caught by nobody — until it is a finding, a clawback, or a qui tam complaint.

BEFORE YOU SPEND ANYTHING

Four Ways to Make the Problem Smaller

Ordered by how much work each one removes. Every one of these is cheaper than the cheapest thing you can buy.

1

Do You Touch CUI at All?

FCI only means Level 1 — 15 requirements, not 110.

2

Where Does It Live?

Process, store, transmit. Limit all three and the boundary shrinks.

3

What Have You Already Done?

Reciprocity — evidence you own that maps to more than one framework.

4

What Has Someone Else Done?

Inheritance and enclaves — controls a provider already operates.

STEPS 1 AND 2

Scope Honestly

Level 1

15

Basic safeguarding requirements — FCI only

Level 2

110

Requirements, 320 objectives — CUI

From the Cohort

One of the six documented a boundary that handles FCI only and does not process CUI — and stopped there, with a written trigger to reassess if a contract introduces CUI.

- Process, store, transmit — limit all three. Every system inside the boundary is assessed, documented, and evidenced *forever*.
- Ask your contracting officer in writing what you will actually receive and how it will be marked. Inconsistent CUI marking is a known problem — you are not being difficult by asking.
- **Over-scoping is the single largest avoidable cost in this program.**

STEP 3

Reciprocity — Work You Have Already Done

Three different things get called reciprocity. Only two of them are real, and mixing them up is expensive.

REAL — CODIFIED

Inheritance

Cloud handling CUI must meet FedRAMP Moderate or equivalency. Your boundary's infrastructure layer inherits from a provider who already documented it. **Inherited still has to be documented as inherited.**

REAL — CONDITIONAL

Evidence Reuse

800-171 is tailored from 800-53, so one evidence set can map both ways — conditional on meeting the strictest parameter. FedRAMP says quarterly where your policy says annually, and the reuse quietly fails.

DOES NOT EXIST

Certification Credit

No formal reciprocity between CMMC and FedRAMP, SOC 2, or ISO 27001. A head start, not a finish line — and your prime knows it.

The reform RFI asked industry directly about leveraging existing capabilities. This is a live question, not a settled one.

STEP 4

Enclave — Work Someone Else Has Already Done

Reciprocity taken to its logical end: move CUI into an already-compliant environment and shrink what has to be assessed at all.

What It Removes

- Collapses assessment scope — often the cheapest true path for a one-CUI-contract shop
- Takes the hardest controls off your plate: boundary protection, audit, encryption
- Turns the job into one question — which controls are yours?

What It Costs

- Recurring subscription, indefinitely
- Migration friction — staff have to actually change how they work
- Inherited controls still require documented inheritance. Inherited is not ignored.
- Confirm the provider's authorization and request the customer responsibility matrix.

The NCODE team is briefing this in depth today — go listen to them.

WHERE TO GET HELP

Six Routes, Ordered by Cost

Most small businesses use two or three of these together.

Free Federal Resources

Project Spectrum · NIST · CISA no-cost cyber hygiene scanning

projectspectrum.io · csrc.nist.gov · cisa.gov

APEX, SBDC, and MEP Advisory

No-cost counseling on which level applies, plus referrals

marylandapex.org · americassbdc.org · nist.gov/mep

Self-Serve Compliance Platforms

Software that maps controls and structures documentation — but the system described must actually exist.

RPOs and Consultants

Registered practitioners who run the gap assessment and remediation. APEX and SBDC can refer you.

Managed Enclave Providers

Move CUI into a compliant environment — see the NCODE brief for specifics.

C3PAO Mock Assessment

A paid rehearsal against the real standard, by someone who assesses for a living.

⚠ A platform will happily write a beautiful SSP describing a system you do not have — and a consultant's work does not transfer your liability. You are still the one signing the affirmation.

THE PART NOBODY MENTIONS

You May Not Be Paying for This Out of Pocket

Compliance Costs Are Allowable Costs

Gap assessments, remediation work, assessment fees, and ongoing compliance program costs are allowable under DoD contracts. If you already hold a contract, that reframes the entire spending conversation.

Watch — Do Not Plan On

Tax-credit legislation for CMMC costs has been proposed but not enacted. Monitor it with your tax advisor — do not budget against it.

Three People Can Answer This Before You Spend Anything

Your Contracting Officer

How compliance costs are treated on your specific award — and what CUI you will actually receive

Your APEX Counselor

Which level applies, and what you can stop doing

Your Tax Advisor

Whether any credit provision has actually been enacted

> The document is not the point. **The truth of the document is the point.**

1 Scope Honestly

Limit process, store, and transmit. Ask your CO in writing what you will actually receive.

2 Verify Before You Document

Pick any requirement in your SSP. Trace it to evidence in under five minutes. If you cannot — that is your finding, and it costs nothing to run.

3 Start Collecting Evidence Now

Point-in-time artifacts across consecutive months cannot be produced retroactively. That is the one thing money cannot fix later.

Questions — and the resource list is yours to keep.

Duane Wilson · Move America · Hanover, MD

U.S. Army's Next-Generation Commercial Operations in Defended Enclaves (NCODE) Team

U.S. ARMY

DES
DATA | ENGINEERING | SOFTWARE

ADASM DES

NCODE | Next-generation Commercial Operations in Defended Enclaves

Defending DIB SBs

26 AUG 2026

Christopher “Glenn” Krueger
NCODE Team Lead
Warfighter Acquisition Support
ASA (ALT) ADASM-(DES) Modernization Protection

Overall Classification: **UNCLASSIFIED**

U.S. ARMY

NCODE Overview

DES DATA | ENGINEERING | SOFTWARE

NCODE is designing a standardized pathway for small businesses in the Defense Industrial Base (DIB) to achieve CMMC at various levels by building a marketplace of verified service providers.

Challenge: Small businesses in the DIB face security risks

- Small businesses struggle to meet cybersecurity requirements due to cost and/or skill gaps
- The DIB is facing increasingly sophisticated attacks from our adversaries, and small businesses are a prime target
- The government cannot sustainably subsidize cost for small businesses
- Commercial solutions available, but SBs face an ambiguous, difficult-to-navigate market.

Action: Build a Marketplace of verified service providers

- ✓ Secure operating environment for DIB partners
- ✓ Savings for SBs at scale
- ✓ Inherited Controls
- ✓ Streamlined pathway to CMMC
- ✓ Tailored capabilities for SBs
- ✓ Consistent, transparent solutions for SBs

NCODE's goal is to reduce SB burden to implement cybersecurity to protect the government's data.

U.S. ARMY

CMMC: a DoW Effort to Secure the DIB

DES DATA | ENGINEERING | SOFTWARE

Cybersecurity Maturity Model Certification (CMMC)

- Developed by the Department of War
- Enhances the protection of Controlled Unclassified Information (CUI) within the Defense Industrial Base (DIB)
- Aligns with the National Institute of Standards & Technology (NIST) cybersecurity guidance in special publications (SP) 800-171 and 800-172.

	CMMC 1	CMMC 2 (Self)	CMMC 2 (Certification)	CMMC 3
Control Requirements	FAR 52.204-21 15 Requirements	NIST SP 800-171 110 Requirements	NIST SP 800-171 110 Requirements	NIST SP 800-171 NIST SP 800-172 111-134 Requirements
Assessment Requirements (Annual Affirmation)	Self (Annual)	Self (every 3 years)	Certified 3rd Party Assessment Organization (C3PAO) every three years	Certified 3rd Party Assessment Organization (C3PAO) every three years DIBCAC Assessment
Applicable Types of Data	FCI	CUI categories outside the Defense Organizational Index Group	CUI in Defense Organizational Index Group. (CTI, DCRIT, NNPI, PSI, DCNI)	CUI associated with advanced technologies Significant aggregation of CUI Ubiquity - when an attack on a single system has widespread effects

U.S. ARMY

How can SBs achieve CMMC Level 2 cost-effectively?

DES DATA | ENGINEERING | SOFTWARE

- According to a draft report from the National Ombudsman, CMMC L2 (Cert) can cost between $348K and $1,190K.
- CMMC-related costs will pass on to the government at a high rate, potentially beyond 100%.
- NCODE is the Department's premier CMMC assistance plan, allowing SBs to save ~80% of costs via secure commercial cloud enclaves.

Option	Lower Cost	Median Cost	Higher Cost	Estimated Savings (80%)
Traditional CMMC L2	$348K	$769K	$1,190K	N/A
CMMC L2 with NCODE	$69.6K	$153.8K	$238K	$278.4K – $952K

U.S. ARMY

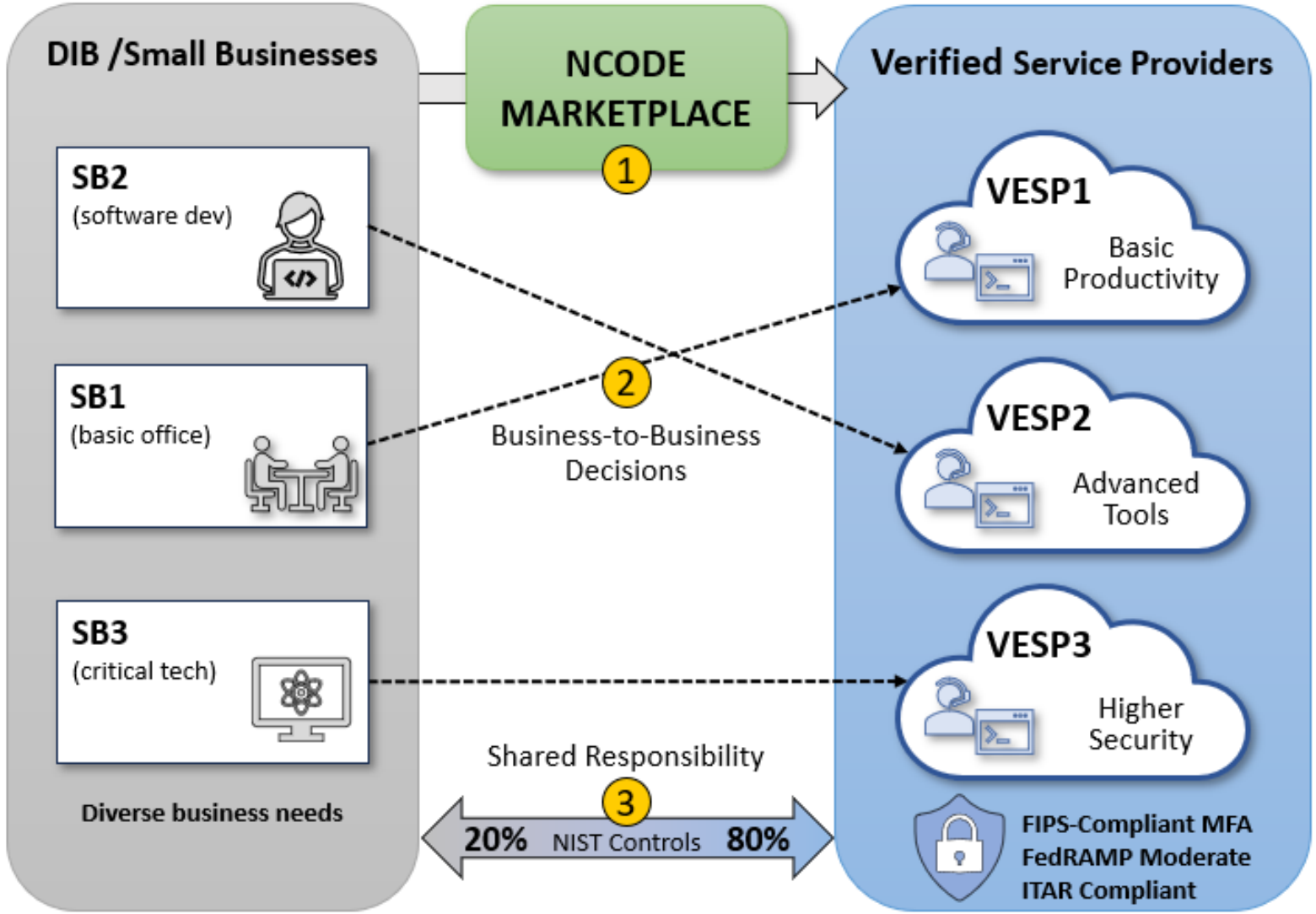
NCODE Commercial Marketplace for SB Security

DES DATA | ENGINEERING | SOFTWARE

1. Government facilitated **marketplace of commercial Verified External Service Providers (VESPs)** with validation and quality assurance

2. DIB/SB chooses VESP based on **individual business needs** (e.g., specialized tools, advanced security, etc.)

3. VESP and SB **share responsibility** for security controls at a **significant cost saving**



U.S. ARMY

NCODE Verified Marketplace for Commercial Solutions to SB Security

DES DATA | ENGINEERING | SOFTWARE

NCODE Supporting Concepts

- Verification: ESPs must pass verification procedures to confirm safety, security, and transparency,
  - FOCI Check
  - Cyber Assurance Document Review
    - Limited Penetration Test (if needed)
  - Vendor Lock Mitigation Survey
  - Cost Transparency Survey
- Control Inheritance: Enables DIB/SBs to inherit up to ~80% of the 110 NIST-171 controls, greatly reducing burden and cost of adherence.
- Assessment Streamlining: Streamlines time and cost of CMMC assessments by building off prior assessments of a CMMC level 2 certified ESP.

NIST 171 Section / Control Family		ALL	BREAKDOWN	
			ESP Coverage	Shared Coverage
3.1	Access Control*	22	16	6
3.2	Awareness & Training	3	0	3
3.3	Audit & Accountability*	9	9	0
3.4	Configuration Management*	9	9	0
3.5	Identification & Authentication*	11	11	0
3.6	Incident Management*	3	0	3
3.7	Maintenance	6	6	0
3.8	Media Protection	9	8	1
3.9	Personnel Security	2	0	2
3.10	Physical Protection	6	5	1
3.11	Risk Assessment**	3	2	1
3.12	Security Assessment**	4	3	1
3.13	System & Configuration Protection	16	16	0
3.14	System & Information Integrity*	7	7	0
	TOTALS	**110**	**92**	**18**
	PERCENTAGE	**100%**	**83%**	**17%**

* Partial control family assessment
** Full control family assessment

U.S. ARMY

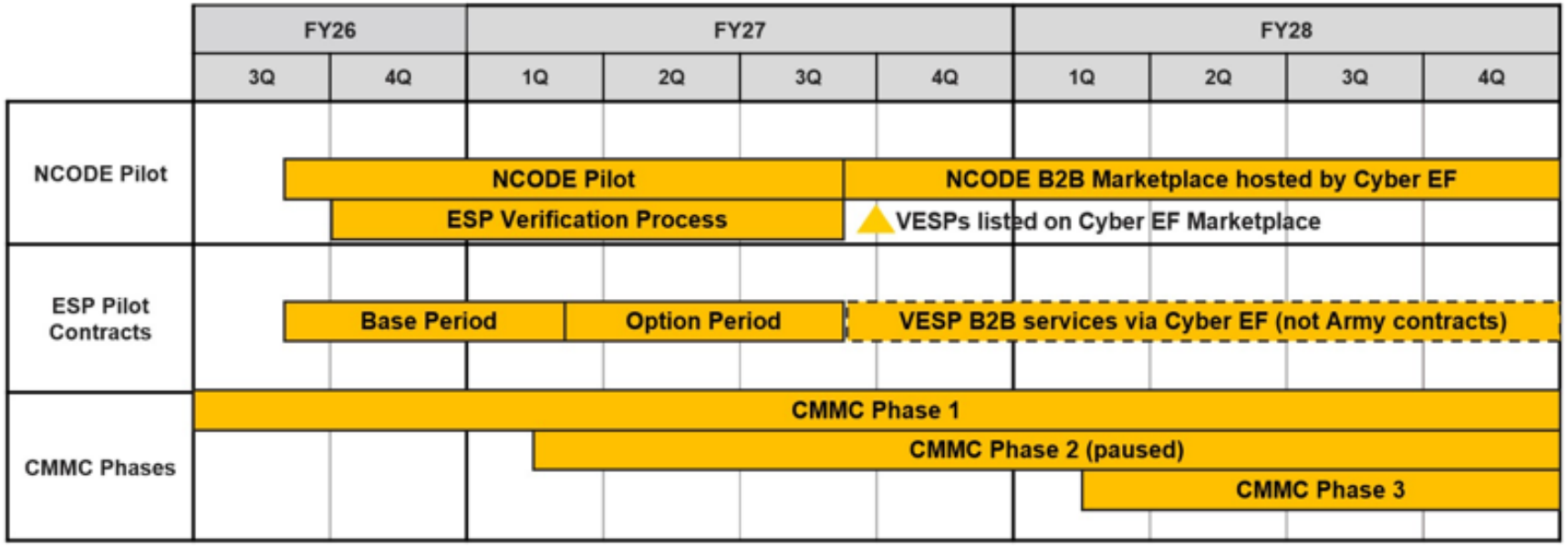
NCODE Pilot Plans

DES DATA | ENGINEERING | SOFTWARE

NCODE Agile Pilot

- The NCODE Pilot is an agile effort that will iterate on the concepts of Verification, Control Inheritance, and Assessment Streamlining
- CPE SBs can have a prominent role in the NCODE Pilot, helping establish baselines and thresholds while achieving CMMC Level 2
- With the addition of the Golden Dome of America (GDA) SBs, NCODE will rapidly bring on additional providers for productivity, DevSecOps, and On-Prem manufacturing tools.

NCODE Pilot Schedule



NCODE Pilot ESPs

Company	Type of Service
ATX Defense	Productivity
Beryllium Infosec	Productivity
Cytex	DSO
David T Scott & Associates	Productivity
Eccalon	DSO
Exostar	Productivity
Security Centric	Manufacturing
Summit 7	Productivity

- These ESPs have not yet been verified.
- NCODE is working to verify and fund all 8 ESPs as the pilot progresses
- ATX Defense and Exostar are funded to onboard GDA SBs

U.S. ARMY

DES
DATA | ENGINEERING | SOFTWARE

Questions?

https://army.mil/ncode
ncode@army.mil

Break

NAVSEA NAVAL SEA SYSTEMS COMMAND | NAVAL SURFACE WARFARE CENTER INDIAN HEAD DIVISION

FUTURE COMMAND-WIDE OPPORTUNITIES - SERVICES

- **Engineering & Technical Services:**
  - Professional Engineering and Technical Support
  - Ordnance and Energetics Support
  - Decontamination and Demilitarization
  - Environmental Remediation
- **Construction & Facilities:**
  - Construction Services (IDIQ MACC, A-E services)
  - Building Repair and Renovation
  - Facilities Management and Support
- **Research & Development:**
  - Naval Energetics Systems and Technologies (NEST)
  - Small Business Innovation Research (SBIR)
  - Experimental Development
- **Maintenance, Repair, and Overhaul:**
  - Maintenance of Equipment (Instruments, Lab Equipment, HVAC)
  - Lease/Rental of Equipment
- **IT & Professional Services:**
  - IT and Telecom Support (Software as a Service, Cloud Environments)
  - Program Management Support

NAVSEA
NAVAL SEA SYSTEMS COMMAND
NAVAL SURFACE WARFARE CENTER
INDIAN HEAD DIVISION

FUTURE COMMAND-WIDE OPPORTUNITIES - MATERIALS

- **Ordnance Components & Hardware:**
  - Rocket and Missile Components (Motors, Nozzles, Fin Kits)
  - Cartridge and Propellant Actuated Devices (CAD/PAD)
  - Warhead Components (Adapters, Cases, Liners)
  - Ammunition and Munitions
- **Chemicals & Energetic Materials:**
  - Bulk Explosives and Propellants (e.g., Otto Fuel II, N5)
  - Acids, Bases, Solvents, and other chemical compounds for production
  - Specialty Chemicals (e.g., Di-butyl Sebacate, Propylene Glycol)
- **Fabricated Parts & Assemblies:**
  - Machined Metal Parts (high-tolerance parts, tubes, housings)
  - Tooling, Carts, and Dollies
- **Specialized Equipment:**
  - Lab and Testing Equipment (Environmental Chambers, Analyzers)
  - IT and Telecom Equipment (Servers, Networking Hardware)
  - Specialized Shipping and Storage Containers
- **Research & Development Materials:**
  - Materials for experimental development and testing

NAVSEA
NAVAL SEA SYSTEMS COMMAND

NAVAL SURFACE WARFARE CENTER
INDIAN HEAD DIVISION

Corporate Operations Department (10)

Dean Heitkamp, Technical Acquisition Specialist

NAVSEA
NAVAL SEA SYSTEMS COMMAND

NAVAL SURFACE WARFARE CENTER
INDIAN HEAD DIVISION

CORPORATE OPERATIONS (10)

10

Enable the Navy's arsenal to create, produce and adapt by providing operational, logistical, and business expertise.

VISION

- To be the Navy's benchmark for agile, innovative, and integrated arsenal operations, trusted logistics, and premiere business solutions
- Corporate Operations is the backbone of NSWC IHD

CAPABILITIES

- Human Resources Management: Talent acquisition, workforce development, employee relations, and compliance with federal employment policies to support mission readiness
- Infrastructure: Oversight of physical assets, maintenance, space planning, and ensuring operational continuity across all facilities
- Information Technology Services: Implementation and maintenance of secure, reliable IT systems, cybersecurity protocols, and data management to enable effective communication and operations
- Security and Intelligence Operations: Protection of personnel, assets, and information through physical security, threat analysis, and coordination with intelligence agencies
- Corporate Planning and Logistics: Strategic resource allocation, supply chain management, and logistics coordination to support efficient operational workflows

WARFIGHTING IMPACT

Corporate Operations directly contributes to warfighting readiness by:

- Create an agile and innovative logistics capability that optimizes resource flow, supporting rapid delivery of solutions and enhancing arsenal responsiveness
- Streamline processes and leverage technology to enhance operational efficiency, ensuring timely delivery of high-quality products and maximizing resource utilization.
- Optimize organizational structure and roles to enhance agility, enabling rapid adaption to emerging requirements and effective delivery of superior energetics solutions

NAVSEA
NAVAL SEA SYSTEMS COMMAND

NAVAL SURFACE WARFARE CENTER
INDIAN HEAD DIVISION

Why CMMC is Critical for Our Partners

- Code 10 directly enables the technical departments—such as Systems Engineering, Energetics Manufacturing, and Explosive Ordnance Disposal—to deliver their mission to the warfighter by providing essential logistical, facility, and administrative support.

- Hardware Sensitivity: Code 10 oversees the procurement and infrastructure for high-security physical assets. This includes hardware for Arms, Ammunition, and Explosives (AAE) Security Upgrades, security door replacements, and the procurement of safes, vaults, locks, and shredders designed for classified material destruction. They also handle the logistics for ordnance handling equipment and specialized machine tools.

- Information Sensitivity: The department processes highly sensitive, mission-critical data, including Controlled Unclassified Information (CUI). This encompasses facility blueprints, security vulnerabilities, multimillion-dollar defense contracts, and Foreign Threat Vulnerability Assessments.

- Additionally, because Code 10 includes Human Resources and Security divisions, they manage sensitive personnel data.

NAVSEA
NAVAL SEA SYSTEMS COMMAND

NAVAL SURFACE WARFARE CENTER
INDIAN HEAD DIVISION

Future Acquisition Opportunities

Brief Description	Anticipated Announcement Date (QTR / FY)	Estimated Dollar Value
Security and IT	3rd QTR/FY 27	> $50M - < $100M
Warehouse and Logistics	3rd QTR/FY 27	> $7.5M - < $50M
Safety Glasses/ Shoes	3rd QTR/FY 27	< $2M
Corporate Communications	3rd QTR/FY 28	> $2M - < $7.5M
NAVSEA Enterprise Resource Planning (ERP) Business Office Support	3rd QTR/FY 27	> $50M - < $100M
Facility Support Services Industrial	4th QTR/FY 26	> $50M - < $100M
Facility Support Services Engineering	4th QTR/FY 26	> $50M - < $100M
Technical Collaboration initiative	3rd QTR/FY 27	> $2M - < $7.5M
Snow Equipment	4th QTR/FY 26	< $2M
Indefinite Delivery / Indefinite Quantity Architect-Engineer Industrial Services	2nd QTR/FY27	> $50M - < $100M
Indefinite Delivery / Indefinite Quantity Architect-Engineer General Design Services	4th QTR/FY 26	> $50M - < $100M
Indefinite Delivery / Indefinite Quantity Architect-Engineer for Mechanical, Electric, and Plumbing Services	2nd QTR/FY27	> $50M - < $100M
Multiple Award Task Order Contract (MATOC), Multiple Award Construction Contract (MACC) in support of targeted facility upgrades, regional construction, and infrastructure repairs, designated as an 8(a) Set-Aside	2nd QTR/FY27	> $50M - < $100M

NAVSEA
NAVAL SEA SYSTEMS COMMAND

NAVAL SURFACE WARFARE CENTER
INDIAN HEAD DIVISION

Contract Categories- Services

Services

- Security
- Warehouse Support
- Facility Support
- Information Technology Support
- Human Resources Support
- Records Management
- Tech Screening / Procurement Cell Services (PROCEL)
- Data Analytic Cell (DAC)

NAVSEA
NAVAL SEA SYSTEMS COMMAND

NAVAL SURFACE WARFARE CENTER
INDIAN HEAD DIVISION

Conclusion & Contact Information

- For any industry-related questions, please contact: Dean Heitkamp at dean.a.heitkamp.civ@us.navy.mil

Research & Engineering Department (E)

Jessica Schombs, Technical Acquisition Specialist

NAVSEA
NAVAL SEA SYSTEMS COMMAND

NAVAL SURFACE WARFARE CENTER
INDIAN HEAD DIVISION

RESEARCH & ENGINEERING (E)

Our Navy's resource for delivery of energetic system solutions across the full acquisition cycle, providing the warfighter with kinetic advantages.

CAPABILITIES	WARFIGHTING IMPACT	LINES OF OPERATION
• Detonation Sciences Experimentation Campus • Advanced prototyping, fabrication, and additive manufacturing of energetic component technology • Underwater Analysis Facility (UWAF) • Electrostatic Discharge (ESD) test facility	• Multi—domain warhead and fuze development from concept to program of record • Advanced energetic test and characterization to tailor lethal effects to targets of interest • Lethal Effects analysis to inform weapon system CONOP/CONEMP • Life-cycle and logistics services for fielded conventional weapon systems and CAD/PADs	• Unmanned System (UxS) kinetic payload development • Novel Energetic Materials formulation and synthesis • Advanced diagnostics, demonstration, test and evaluation of energetic components • Advanced prototyping, fabrication, and additive manufacturing of energetic components

NAVSEA
NAVAL SEA SYSTEMS COMMAND

NAVAL SURFACE WARFARE CENTER
INDIAN HEAD DIVISION

Why CMMC is Critical for Our Partners

Capability	Why CMMC is Necessary
Detonation Sciences Experimentation Campus	Protects sensitive explosive data and test results from cyber threats.
Advanced prototyping, fabrication, and additive manufacturing	Safeguards technical data and intellectual property for energetic components.
Underwater Analysis Facility (UWAF)	Secures sensitive analysis and operational data.
Electrostatic Discharge (ESD) test facility	Prevents exploitation of safety and reliability data.
Multi-domain warhead and fuze development	Protects full lifecycle weapon system data.
Advanced energetic test and characterization	Secures data/models for tailored lethal effects.
Lethal Effects analysis	Protects operational concepts and TTPs.
Life-cycle and logistics services	Secures maintenance, supply chain, and operational data.
UxS kinetic payload development	Protects advanced unmanned system payload data.
Novel Energetic Materials formulation	Safeguards research and synthesis methods.
Advanced diagnostics, demonstration, test and evaluation	Protects performance and safety validation data.

- CMMC level required for most Research and Engineering Department contracts is CMMC Level 2.

NAVSEA
NAVAL SEA SYSTEMS COMMAND

NAVAL SURFACE WARFARE CENTER
INDIAN HEAD DIVISION

Future Acquisition Opportunities

Brief Description	Anticipated Announcement Date (QTR / FY)	Estimated Dollar Value
Operations Support	FY26-27	> $7.5M - < $50M
Chemicals	FY26-27	> $7.5M - < $50M
Engineering Services Support	FY26-FY27	> $100M - < $250M
Shipping Containers	4th QTR/FY 26 & 27	> $2M - < $7.5M

NAVSEA
NAVAL SEA SYSTEMS COMMAND

NAVAL SURFACE WARFARE CENTER
INDIAN HEAD DIVISION

Conclusion & Contact Information

- CMMC is necessary for these capabilities because they all involve handling, generating, or storing Controlled Unclassified Information (CUI) or other sensitive defense information. The loss or compromise of this information through cyber means could directly impact U.S. warfighting capability, technological advantage, and national security. CMMC provides a standardized framework to ensure that all contractors and partners implement adequate cybersecurity to protect this critical information throughout the defense supply chain

- POC: Jessica Schombs, Technical Acquisition Specialist
  - Email: Jessica.m.schombs.civ@us.navy.mil

Energetics Manufacturing Technology Department (M)

Normary Camacho-Cardoza, Technical Acquisition Specialist

NAVSEA
NAVAL SEA SYSTEMS COMMAND

NAVAL SURFACE WARFARE CENTER
INDIAN HEAD DIVISION

ENERGETICS MANUFACTURING TECHNOLOGY (M)

Produces and delivers unsurpassed quality energetics for the Nation's strategic deterrence posture and provide a decisive advantage across all domains to operational and tactical military commanders executing operations across the conflict continuum.

CAPABILITIES

- Producing large and small-scale rocket motors and military munitions
- Scale-up of novel energetics for future use in large scale production
- Testing of components, chemical ingredients, and products to support energetics production and fleet use
- Manufacturing Cartridge Actuated and Propellant Actuated Devices for aircrew escape systems
- Machining, welding, and tooling of munitions components
- Over the road transportation of explosives anywhere in the continental United States

WARFIGHTING IMPACT

- Ensuring warfighter readiness by providing reliable explosives and propellants and reducing supply chain disruptions
- Rapid prototyping and transition of new energetics to enhance lethality and performance
- Strategically shifting production lines to align munitions output with current operational demands and the evolving threat landscape, ensuring a proactive and adaptive defense posture

LINES OF OPERATION

- Scalable Mix, Cast, Cure Production
- Various size energetic pressing capabilities
- Extruded Product Manufacturing
- Novel processing techniques
- Full suite of Test and Evaluation capabilities
- Safe, reliable and efficient energetics logistics support

NAVSEA NAVAL SEA SYSTEMS COMMAND | NAVAL SURFACE WARFARE CENTER INDIAN HEAD DIVISION

Contract Categories- Services

- M Department contracts for a wide range of services to support our critical manufacturing and engineering missions across the following sectors:
  - Engineering & Technical Support (Decontamination/Demilitarization, Operations)
  - Maintenance, Repair, and Rebuild of Equipment (Instruments, Lab Equipment, Metalworking Machinery, Photographic Equipment, Heating, Ventilation, and Air Conditioning(HVAC).
  - Information Technology (IT) and Telecom Support Services (Software, Cloud Environments)
  - Logistics and Ordnance Inventory Management Support
  - Wastewater Treatment and Environmental Remediation
  - Lease or Rental of Equipment

NAVSEA
NAVAL SEA SYSTEMS COMMAND
NAVAL SURFACE WARFARE CEN...
INDIAN HEAD DIVISION

Contract Categories- Materials

- M Department also procures a variety of raw materials and fabricated parts, such as:
  - **Chemicals:** Acids (Nitric, Sulfuric), Bases (Sodium Hydroxide), Oxidizers (Ammonium Perchlorate), Solvents, Amines, and Polyols.
  - **Bulk Explosives & Propellants:** Including N5 Propellant and Otto Fuel II ingredients.
  - **Metal Parts & Components:**
    - Large-scale rocket motor components and tubes
    - Small, high-tolerance machined parts (lathe parts, cups, pins)
    - Components for CAD/PAD
  - **Containers & Packaging:** Specialized shipping containers, drums, and packaging materials (foam, desiccants).
  - **Equipment:** Forklifts, carts, dollies, and various types of testing and lab equipment.

NAVSEA
NAVAL SEA SYSTEMS COMMAND

NAVAL SURFACE WARFARE CENTER
INDIAN HEAD DIVISION

Future Acquisition Opportunities

Brief Description	Anticipated Announcement Date (QTR / FY)	Estimated Dollar Value
Ordnance Services Support	2nd QTR / FY27	> $100M - < $250M
Manufacturing & Services Acquisition (MASA) Manufacturing Support (Machine Shops)	2nd QTR / FY26	> $7.5M - < $50M
OTTO Fuel Production - 5 year	2nd QTR / FY26	> $7.5M - < $50M
Engineering Support for Decon/Demil	3rd QTR / FY26	> $7.5M - < $50M
Di-butyl Sebacate (DBS) Large 5 Year	2nd QTR / FY26	> $7.5M - < $50M
MK22 HEAD CAPS	4th QTR / FY26	> $2M - < $7.5M
MK70 Ballast Kits	2nd QTR / FY26	> $2M - < $7.5M
PA92 Containers	2nd QTR / FY26	> $2M - < $7.5M
1,3,5-Trichlorobenzene(TCB) // 5yr Contract	2nd QTR / FY27	> $2M - < $7.5M
N5 Propellant	2nd QTR / FY27	> $2M - < $7.5M
JAU-8 equipment	2nd QTR / FY26	> $2M - < $7.5M
Shielded Mild Detonating Cord (SMDC) Test Tips	2nd QTR / FY27	< $2M
Nitric Acid(98%+) // 5yr Contract	2nd QTR / FY27	< $2M
Universal Bomb Dolly	4th QTR / FY26	< $2M
IMSUS Charge Holder and Tail Fin Assembly	4th QTR / FY26	< $2M

NAVSEA
NAVAL SEA SYSTEMS COMMAND

NAVAL SURFACE WARFARE CENTER
INDIAN HEAD DIVISION

Conclusion & Contact Information

- CMMC compliance is not just a future requirement; it is a present-day necessity for partnering with the Department of War. Ensuring the security of our supply chain is critical to the M Department's mission and to the safety of the warfighter. We are committed to working with our small business industry partners to navigate these requirements and ensure our collective success. We encourages all potential and current vendors to begin their CMMC journey now.

- Point of Contact: For industry questions for the Manufacturing Department, please contact Normary Camacho Cardoza at normary.b.camachocardoza.civ@us.navy.mil.

Warfighter Defense & Systems Integration Department (W)
Explosive Ordnance Disposal (EOD) Management Division
EOD Systems Division
Battle Lab Division

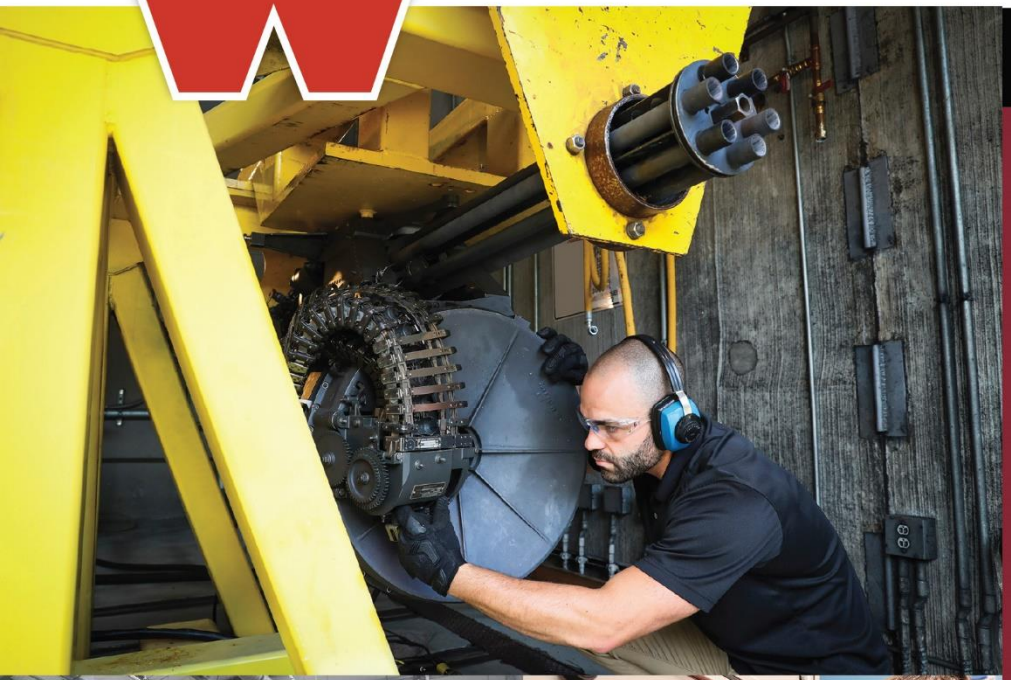
Jose Ramirez, Technical Acquisition Specialist

NAVSEA
NAVAL SEA SYSTEMS COMMAND

NAVAL SURFACE WARFARE CENTER
INDIAN HEAD DIVISION

WARFIGHTER DEFENSE & SYSTEM INTEGRATION (W)

Provides world class support to the Warfighter in the areas of guns, ammunition, chemical biological radiological defense, and explosive disposal (EOD) tools, technology and information. Also, provide packaging, handling, storage and transportation (PHST) solutions that meet or exceed the needs of our warfighters.



CAPABILITIES

- Chemical Biological and Radiological Defense (CBRD) filter media laboratories, collective protection test-bed, CONUS/OCONUS repair facilities, and CBR littoral testing lab (in-progress)
- Explosives chemistry, electronics and prototyping labs, disassembly complex, and explosives test and robotics ranges
- Medium caliber live-fire test range facility, minor caliber lab, gun stand complex and PHST Test facility

WARFIGHTING IMPACT

- Shipboard and Facility CBRD information, systems, testing, installation, maintenance and repair
- EOD information, systems, testing, maintenance and repair
- Gun Weapon System and ammunition packaging, handling, storage, transport, installation, maintenance, and repair
- Direct warfighter support for guns, CBRD and EOD

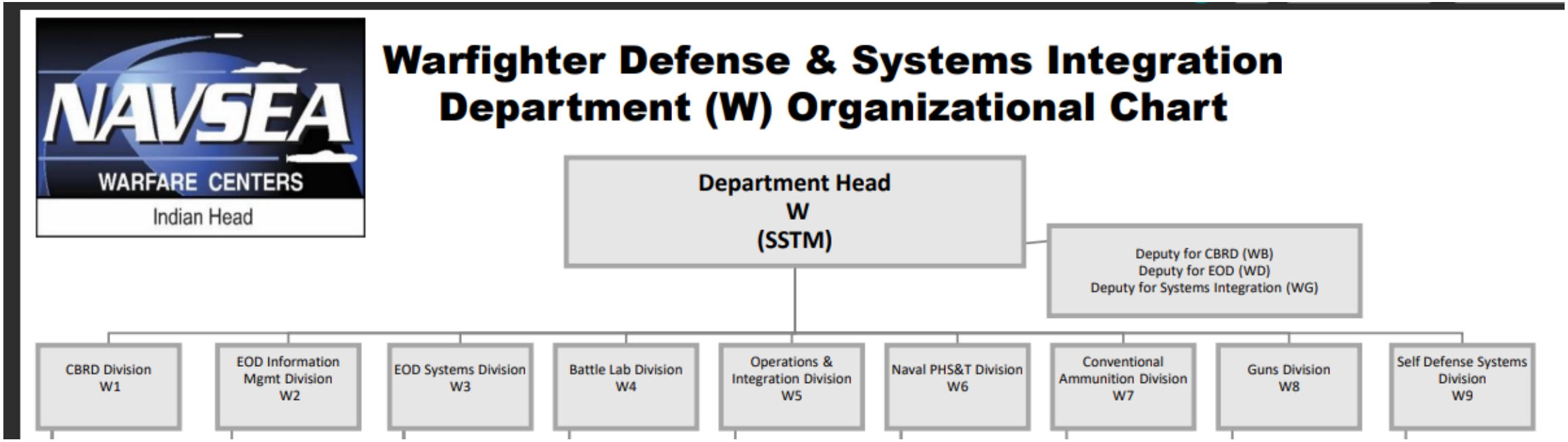
LINES OF OPERATION

- Research Development Test and Evaluation (RDT&E), design agent, and engineering lead for CBR detection, modeling, collective protection, information systems, and medical systems
- RDT&E and engineering lead for EOD detection equipment, publications, unmanned systems, technology assessments, foreign material acquisition and exploitation
- Weapons and armament PHST design agent, in-service and acquisition engineering agent

NAVSEA
NAVAL SEA SYSTEMS COMMAND

NAVAL SURFACE WARFARE CENTER
INDIAN HEAD DIVISION

Warfighter Defense & Systems Integration Department (W)



The Warfighter Defense & Systems Integration Department (W) is a diverse organization comprised of nine divisions, each with a unique mission supporting NAVSEA's objectives. Our capabilities range from Chemical, Biological, and Radiological Defense (CBRD) to Conventional Ammunition and Self-Defense Systems. Given the breadth of our work, this presentation will highlight specific programs and opportunities from a select group of our divisions.

NAVSEA NAVAL SEA SYSTEMS COMMAND | NAVAL SURFACE WARFARE CENTER INDIAN HEAD DIVISION

Deputy Department Overview

WD - EODTECHCEN Mission

Develop and deliver Explosive Ordnance Disposal (EOD) ***knowledge, tools, equipment, their life cycle support*** through an expeditionary work force that ***exploits technology and information, contributes to the technical intelligence process and provides expertise*** which meets the needs of the Department of War **EOD community**, combatant commanders and our interagency partners.

Policy & Instruction for EOD Technology Center:

- **Per DoD Directive 5160.62E, November 8th, 2021, (orig. 1971)**
  - **Designates the Secretary of the Navy (SECNAV) as the DoD Executive Agent (EA)** for Explosive Ordnance Disposal (EOD) Technology and Training (EODT&T)
  - Establishes and maintains an **EOD Technology Center** and a training school in coordination with the Secretaries of the other Military Departments.
  - The EOD Technology Center provides scientific and engineering knowledge and facilities to:
    - Develop, test, evaluate, and integrate equipment and technologies required to provide joint-Military Service EOD capabilities, including the providing of logistics support as applicable.
    - Provide foreign ordnance collection, exploitation, and recovery; ordnance disassembly, intelligence analysis, and engineering; and EOD disposal and render-safe procedures development, testing, maintenance, and distribution.

- **SECNAVINST 5410.118, February 6th, 2023**
  - Establish and maintain the EOD Technology Center (EODTECHCEN) within NSWC IHD. EODTECHCEN is the primary technology execution component of the EODT&T Program. The EODTECHCEN shall:
    - Provide qualified staff to research, design, develop, test, evaluate, and provide in-service and life-cycle support for EOD tools and equipment.
    - Maintain data repository and distribution system for EOD information
    - Provide qualified technical staff to provide foreign ordnance collection, exploitation, recovery, ordnance disassembly, intelligence analysis, engineering, and EOD render safe and disposal procedures development, testing, maintenance, and distribution.
    - Provide liaison with U.S. intelligence agencies
    - Provide an EOD International Programs Office
    - Provide technical and intelligence subject matter expert support to the EOD training school,
    - Serve focal point for EOD technology and technical data efforts executed under the EODT&T Program

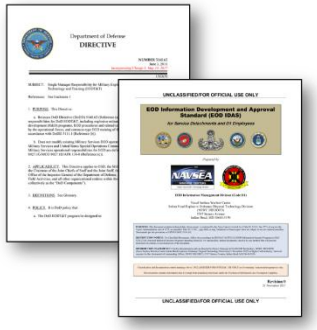
NAVSEA
NAVAL SEA SYSTEMS COMMAND

NAVAL SURFACE WARFARE CENTER
INDIAN HEAD DIVISION

EODTECHCEN
EOD Information Management Division

- **Key Products:** EOD Information Products, Technical Support Center, Render Safe Procedures/TTP development, and FMA/FME, support for Mobile Field Kit/Decision Support System

- **Key Facilities:**
  - Disassembly complex
  - Explosive Test Range 3
  - Main magazine complex
  - Radiography
  - Technical Support Center
- **DODD 5160.62**
- **EOD Information Development & Approval Standards (EOD IDAS)**



NAVSEA
NAVAL SEA SYSTEMS COMMAND

NAVAL SURFACE WARFARE CENTER
INDIAN HEAD DIVISION

EODTECHCEN
EOD Systems Division

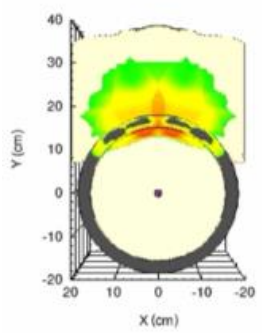
Key Program/Project Areas:

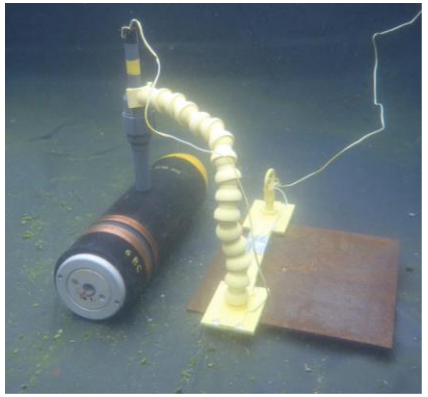
- Detection and Diagnostics
  - Sensors/X-Ray
  - Counter-Improvised Explosive Devices (IED)
  - CREW/Electronics Exploitation
- Maritime Systems
  - Underwater EOD
  - Magnetometer/LoMu
- Unmanned Systems
  - Robotics/UxS
  - AI/Autonomy & Integration
- Energetic Tools and Remediation
  - Ordnance Disrupt/Modeling & Simulation
  - Unexploded Ordnance Clearance Quality Assurance (UXO clearance QA)
- Force Protection Systems
  - Anti-Terrorism/Force Protection
  - EOD Foreign Military Sales
- Material Management
  - Warehousing/Supply Support/Logistics
  - Naval Supply Systems Command (NAVSUP) Weapon Systems Support (WSS) Inventory Control Point (ICP)
- Manufacturing/Prototyping

Support Across the Development Spectrum: Science and technology, prototyping and integration, POR development, T&E, engineering agent/ISEA, non-traditional support/sustainment.








NAVSEA
NAVAL SEA SYSTEMS COMMAND

NAVAL SURFACE WARFARE CENTER
INDIAN HEAD DIVISION

EODTECHCEN
Battle Lab Division

The Battle Lab conducts operational experiments, demonstrations and assessments of existing and emerging technology to feed capability gap assessment, buying decisions and inform requirements development and technology implementation

Assessing the market for viable solutions

Providing actionable information for fielding decisions

Driving future technology development

BATTLE LAB

Industry & Gov't Partnerships

- United States Bomb Technician Association (USBTA)
- Customs and Border Protection (CBP) Memorandum of Understanding (MOU) and Interagency Agreement (IAA).Expeditionary Exploitation Unit One (EXU-1) Memorandum of Agreement.
- Naval Energetic Systems and Technologies (NEST) Other Transaction Agreement (OTA)
- Tech Bridges
- One Warfare Center Team

Demonstration and Assessment Team (DAT)

Integration of warfighter inputs with developmental

Explosive Detection Equipment (EDE)

Evaluation of systems to detect or ID explosives and threats

EOD Technology Assessment (ETA)

Evaluation of emerging & available technology for EOD

NAVSEA
NAVAL SEA SYSTEMS COMMAND

NAVAL SURFACE WARFARE CENTER
INDIAN HEAD DIVISION

Future Acquisition Opportunities

Below is the projected contract forecast for the upcoming fiscal years, focusing on critical EOD systems engineering and sustainment packages.

Project/Contract Title	Brief Description	Anticipated Announcement	Estimated Dollar Value
EOD Services Support Contract	Technical Information development/management, system engineering and logistics, technology assessment and integration	QTR 2/FY 27	> $50M - < $100M

NAVSEA
NAVAL SEA SYSTEMS COMMAND

NAVAL SURFACE WARFARE CENTER
INDIAN HEAD DIVISION

Conclusion & Contact Information

- CMMC certification ensures basic practices compliance for safeguarding Federal Contract Information (FCI), as such, certification is essential to ensure small business remain eligible to be awarded and are able to support requirements.

- WD POC: Jose H. Ramirez, Technical Acquisition Specialist

  Email: jose.h.ramirez4.civ@us.navy.mil

NAVSEA
NAVAL SEA SYSTEMS COMMAND

NAVAL SURFACE WARFARE CENTER
INDIAN HEAD DIVISION

Chemical, Biological, and Radiological (CBR) Defense Division

Vycki Borgnis, Technical Acquisition Specialist

NAVSEA
NAVAL SEA SYSTEMS COMMAND

NAVAL SURFACE WARFARE CENTER
INDIAN HEAD DIVISION

WB Deputy Department Overview

WB Mission & Key Functions

Chemical, Biological, and Radiological (CBR) Defense (WB) at NSWC IHD serves the DoD and the Nation as the Navy Organization providing innovative, timely, and effective products, technical solutions, and expertise in Chemical, Biological, and Radiological Defense.

Key Functions:

- **Information Systems & Applied Research:** Focused on data systems, modeling & simulation, and Next Generations CBRD systems.
- **CBR Collective Protection Systems:** Designing, improving, and sustaining systems that protect personnel in contaminated environments.
- Chemical, Biological, and Radiological Defense (**CBRD) Equipment Integration & Lifecycle Management:** Comprehensive approach to managing CBRD equipment from R&D through testing, fielding, sustainment,
- **CBRD Detection Systems:** Developing and maintaining systems for detecting chemical and biological hazards..
- **Direct Warfighter Support:** Providing rapid training, tailored support, and equipment deployment directly to operational units.

Role within NSWC IHD

Chemical, Biological, and Radiological Defense at NSWC IHD serves as the principal technical authority and lifecycle manager for advanced protection, detection, and information systems, delivering seamless support from initial research and development through testing, deployment, and active sustainment to ensure the warfighter remains protected in all operating environments.

NAVSEA
NAVAL SEA SYSTEMS COMMAND
NAVAL SURFACE WARFARE CENTER
INDIAN HEAD DIVISION

Why CMMC is Critical for Our Partners

Warfighting Impact & Partnership

Warfighter survival in contaminated environments relies on robust CBR defense capabilities. Our industry partners design, build, and maintain the critical sensors and protective equipment that shield our forces. Any compromise in this supply chain threatens to neutralize these defensive capabilities when they are needed most.

Sensitivity of Information & Hardware

Our work involves CUI relating to vulnerability assessments, threat thresholds, and system performance limits. Compromise of this data allows adversaries to engineer countermeasures.

Physical Hardware: Prototyping materials and filtration media designs are strictly controlled to prevent reverse engineering.

Foreseen CMMC Levels

Based on the handling of CUI and critical military hardware designs:

- CMMC Level 2 (Advanced): Will be the standard baseline requirement for the majority of WB/W1 typical contracts involving engineering design, prototyping, and systems integration.
- CMMC Level 1 (Foundational): Reserved strictly for basic COTS service and supply providers

NAVSEA
NAVAL SEA SYSTEMS COMMAND
NAVAL SURFACE WARFARE CENTER
INDIAN HEAD DIVISION

Future Acquisition Opportunities

Below is the projected contract forecast for the upcoming fiscal years, focusing on critical CBR systems engineering and sustainment packages.

Project/Contract Title	Brief Description	Anticipated Announcement	Estimated Dollar Value
CBRD Systems Engineering Support	Full lifecycle engineering, integration, and logistics support for CBR defense systems.	QTR 1/FY27	> $7.5M - < $50M
Specialized Detection Hardware	Development and low-rate initial production of chemical detection sensors.	QTR 3/FY27	> $7.5M - < $50M
Filtration Media Sustainment	Manufacturing and supply of specialized gas and particulate filtration filters.	QTR 2/FY28	> $2M - < $10M

NAVSEA
NAVAL SEA SYSTEMS COMMAND

NAVAL SURFACE WARFARE CENTER
INDIAN HEAD DIVISION

Contract Categories - Services

Typical services contracted by WB/W1 to support our mission requirements include:

Service Category	Description of Required Services
Field Engineering & Fleet Support	Installation, removal, and modification of equipment on afloat and ashore assets (AIT support), fleet readiness assist visits (RAVs), and emergent technical assistance.
Centralized Asset Management	Inventory management, inspection, maintenance, repair, procurement, storage, and shipping for all CBRD, Damage Control/Fire Fighting (DC/FF), Pentagon Force Protection Agency (PFPA), Radiological Controls (RADCON), and EOD programs.
Engineering & Systems Integration	Research, Development, Test, and Evaluation (RDT&E), design, development, integration, and testing of CBRD equipment, including resolving system interface issues and Human Systems Integration (HSI).
Technical Data & Logistics	Development and maintenance of technical data packages (TDPs), engineering drawings, technical manuals, Integrated Logistics Support (ILS), and configuration management.

NAVSEA
NAVAL SEA SYSTEMS COMMAND

NAVAL SURFACE WARFARE CENTER
INDIAN HEAD DIVISION

Contract Categories - Services

Typical materials, components, and hardware procured to support defense operations include:

Material Category	Examples of Required Procurements
CBR Filtration Media	Active carbon components, particulate filters, and custom protective seal materials.
Detector Components	Sensor arrays, specialized circuit boards, and calibration equipment.
Personal Protective Equipment Assemblies	Protective suits, boots, masks, and specialized self-contained breathing apparatus (SCBA) parts.
Test Rig Materials	Calibration gases, aerosol generators, and environmental testing chamber parts.

NAVSEA
NAVAL SEA SYSTEMS COMMAND

NAVAL SURFACE WARFARE CENTER
INDIAN HEAD DIVISION

Conclusion & Contact Information

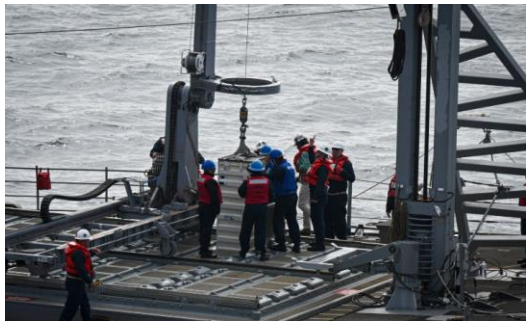
- WB POC: Vycki Borgnis, Technical Acquisition Specialist
  Email: victoria.d.borgnis.civ@us.navy.mil

NAVSEA
NAVAL SEA SYSTEMS COMMAND

NAVAL SURFACE WARFARE CENTER
INDIAN HEAD DIVISION

W8 Guns Division

Ben Herring, W81 Lead Contracting Officer Representative (COR)



NAVSEA
NAVAL SEA SYSTEMS COMMAND

NAVAL SURFACE WARFARE CENTER
INDIAN HEAD DIVISION

Department Overview

Picatinny Detachment Mission

To safely and efficiently transform customer requirements into highly effective, sustainable gun weapon systems; enabling the DoW, joint forces, and foreign military sales (FMS) partners to achieve battlefield supremacy.

W8 Guns Division Focus

Serving as the Navy's premier in-service engineering agent (ISEA), NSWC IHD Picatinny Detachment delivers full-lifecycle logistics and technical support for minor, medium, and major caliber naval gun weapon systems.

* Bridging the gap between *initial requirements* and **sustainable fleet capabilities**.

Core Capabilities

- System installation, troubleshooting, maintenance, repair, overhaul, and modernization
- Comprehensive lifecycle logistics, technical documentation development, and configuration control
- Specialized gun weapon system test and evaluation test and evaluation (T&E)
- Hands-on technical training to prepare Sailors for operational success

NAVSEA
NAVAL SEA SYSTEMS COMMAND
NAVAL SURFACE WARFARE CENTER
INDIAN HEAD DIVISION

Why CMMC is Critical for Our Partners

- Under the Secretary of War's Acquisition Transformation System (ATS) directives, NSWC IHD W Department is pivoting to accelerate the fielding of capabilities to the warfighter:
  - Operational Impact of a Breach: A cyber breach or ransomware attack on a key supplier of gun mounts, barrels, or electronic firing components can instantly halt overhauls and delay ship deployments.
  - Proactive Defense: CMMC shifts vendors from "point-in-time" self-attestation to continuous, verified cyber readiness
  - Ensuring that production schedules remain uninterrupted, directly supporting fleet operational readiness.
- The CMMC Role: CMMC Level 2 alignment (equivalent to NIST SP 800-171) ensures that W8 division's contractors, subcontractors, and support vendors have verified cyber controls to prevent adversaries from exfiltrating these designs to replicate or disable U.S. Naval gun capabilities

NAVSEA
NAVAL SEA SYSTEMS COMMAND

NAVAL SURFACE WARFARE CENTER
INDIAN HEAD DIVISION

Contract Categories

- W8 ISEA workload includes;
  - Procurement of Gun Weapon Systems (GWS), i.e. MK-45, MK-38, MK-110, MK-46
  - Services (Level of Effort), Engineering & Technology Related Services
  - Spares purchases – for GWS(s)
  - OTA's for Prototyping & developmental items
  - Simplified Acquisition purchases – Software, Hardware, GWS related
  - Indefinite Delivery, Indefinite Quantity (IDIQ)
  - Basic Ordering Agreements (BOA)
  - Fielding Support, i.e. technical support on deck plates, Pierside, etc.
    - On board Technical Assistance (OBTA)
    - Rapid Acquisition and fielding support

NAVSEA
NAVAL SEA SYSTEMS COMMAND

NAVAL SURFACE WARFARE CENTER
INDIAN HEAD DIVISION

W8 Contract Forecast

Future Contract Actions (planned) for FY'27:

Gun Weapon System	Type	Description
MK-15 (CIWS)	IDIQ (Service & Parts)	CIWS AIT FY'27 – FY'32
MK-45	Production & Engineering Services	MK-45 BOA follow on
MK-110	IDIQ (Hybrid)	MK-110 BOA follow on
MLG-27	Parts/Spares & Services	Follow on Requirement
MK-45	Velocimeter spares purchase	Supporting MK-45 Portfolio
All	SAP Purchases	Spontaneous

* Exploring competitive individual procurements where NSWC IHD Picatinny owns the Technical Data Package, even if by part only.

NAVSEA
NAVAL SEA SYSTEMS COMMAND

NAVAL SURFACE WARFARE CENTER
INDIAN HEAD DIVISION

W8 Portfolio

MK38, MK46, MK110, MK45, MK75, MK11

NAVSEA
NAVAL SEA SYSTEMS COMMAND

NAVAL SURFACE WARFARE CENTER
INDIAN HEAD DIVISION

Conclusion & Contact Information

- CMMC certification is a non-negotiable gateway for supporting the W8 Guns Division; contractors without it are legally prohibited from receiving the Controlled Unclassified Information (CUI)—such as Technical Data Packages, blueprints, and repair schematics—required to bid on, manufacture, sustain, or Modernize U.S. Naval Gun Weapon Systems

- W8 POC: Benjamin R. Herring, Technical Acquisition Specialist
- Email: Benjamin.r.herring2.civ@us.navy.mil

Expeditionary Exploitation Unit ONE (EXU-1)

Donna Murphy, Technical Acquisition Specialist

NAVSEA
NAVAL SEA SYSTEMS COMMAND

NAVAL SURFACE WARFARE CENTER
INDIAN HEAD DIVISION

EXU-1 Purpose and Mission

- Expeditionary Exploitation Unit ONE (EXU-1) is a Type II Sea duty technical exploitation command subordinate to NSWC IHD, aligned under Naval Sea Systems Command (NAVSEA).

- The core mission of EXU-1 is to collect, process, exploit, and analyze improvised, conventional/advanced weapons systems, sensor systems, critical infrastructure, and foreign materiel on land and at sea.

NAVSEA
NAVAL SEA SYSTEMS COMMAND
NAVAL SURFACE WARFARE CENTER
INDIAN HEAD DIVISION

Contract Categories- Services/Materials

- Engineering & Technical Support
- Instruments and Equipment maintenance and repair
- IT and Telecom Support Services
- Logistics and Ordnance Inventory Management Support
- Lease or Rental of Equipment
- Training: Non-standard Pre-deployment currently not offered by traditional Navy EOD units.

- Laboratory Instruments and materials
- Various Chemicals
- Power Equipment
- Testing Equipment
- Containers and Packaging/Shipping Materials

NAVSEA
NAVAL SEA SYSTEMS COMMAND

NAVAL SURFACE WARFARE CENTER
INDIAN HEAD DIVISION

Conclusion & Contact Information

- POC: Donna Murphy, Technical Acquisition Specialist

- Email: donna.m.murphy49.civ@us.navy.mil

NAVSEA
NAVAL SEA SYSTEMS COMMAND

NAVAL SURFACE WARFARE CENTER
INDIAN HEAD DIVISION

NSWC IHD
Cybersecurity Maturity Model Certification (CMMC) Virtual Industry Day
Thank You!!!

NAVSEA
NAVAL SEA SYSTEMS COMMAND

NAVAL SURFACE WARFARE CENTER
INDIAN HEAD DIVISION

- Please take the survey at the following link: https://forms.osi.apps.mil/r/vrtUy6WRZS?origin=lprLink

- The presentation slides from todays CMMC Virtual Day will be posted to: https://www.navsea.navy.mil/Home/Warfare-Centers/NSWC-Indian-Head/Partnerships/Small-Business/