The Digital Manufacturing Institute

MxD
REQUEST FOR PROPOSAL

Organic Industrial Base Technology Enhancement Recommendation for Cyber Hardening (OIB Tech)

Revision 1.0 Release Date: October 22 2026

Project Contact: **Patrick Barrett**

Sr. Project Manager

Patrick.Barrett@mxdusa.org

Technical Contact: **Emily Shanker**

Mgr System Integration, Engineering

Emily.Shanker@mxdusa.org

MxD
1415 North Cherry Ave
Chicago, IL 60642

TABLE OF CONTENTS

I. Record of Change 4
II. Timeline and Project Constraints 4
III. Introduction 4
IV. Technical Summary 7
Problem Statement 7
Overview and Background 7
Objectives 7
Requirements 8
General Requirements 8
Current State Assessment 9
Architecture Definition and Engineering Development 10
System Integration and Commissioning 11
Demonstration, Validation and Transition 11
Roles and Responsibilities (RACI) 12
Out of Scope 12
V. Program Requirements 15
Program Management 15
Funding Requirements 15
Travel, Facility Access and Insurance Requirements 15
Period of Performance Requirements 15
Ownership of Deliverables and Intellectual Property 15
VI. Eligibility 16
MxD Membership 16
Notification of Participation Non-U.S. Citizens 17
VII. PROPOSAL Evaluation 17
Evaluation Process for Project Calls 17
Evaluation Criteria 17
Submission Details 18
VIII. Next Steps 18
Notification 18
Final Revisions 18
Contract 18

I. APPENDIX A 19
Use Case Feasibility and Equipment Mapping Matrix 19
II. APPENDIX B 20
Use Case Examples (information purposes only) 20
Data Driven Programming (Before) 20
Active Process Monitoring (During) 20
Adaptive Quality Feedback (After) 20
Operational Metrics (OEE) 21
III. APPENDIX C 22
OT Controls 22
Disqualifying controls/findings for connected Operation Technology (OT) systems 22
Unsupported SW/HW 22
PPSM 22
IV. APPENDIX D 23
Control System/OT Security Architecture 23

I. RECORD OF CHANGE

Revision	Date	Sections	Description
1.0	October 22	N/A	Original

II. TIMELINE AND PROJECT CONSTRAINTS

Deadline for submissions to be received	November 13, 2026
Public Webinar Information Session 1	10:30am CT, November 5, 2026
Public Webinar Information Session 2	10:30am CT, November 12, 2026
Follow up clarification meetings as needed	Throughout the submission phase
Feedback to participants	By December 07, 2026
Anticipated MxD Funding	$2,700,000
Period of Performance	24 Months (maximum)

III. INTRODUCTION

MxD: The Digital Manufacturing Institute strengthens U.S. economic prosperity and national security by driving digital adoption in manufacturing. In partnership with the Department of War (DOW), MxD (also referred to as the Institute) equips U.S. factories with the digital tools and expertise required for modernization. MxD's core mission is to strengthen U.S. manufacturing global competitiveness to advance economic prosperity and national security by accelerating digital adoption, securing supply chains, and empowering the workforce.

MxD has invested over $450 million in more than 212 applied research and development projects in areas including design, product development, systems engineering, factory modernization, agile and resilient supply chains, workforce training, and cybersecurity.

MxD is also the DOW's National Center for Cybersecurity in Manufacturing. All MxD projects must take cybersecurity into consideration.

This RFP is publicly available on the MxD website at https://members.mxdusa.org/page/project-calls. This public posting represents the official notification of a request to submit the required documents. Amendments to an MxD RFP may be used to extend due dates, clarify procedural requirements, or modify technical requirements. If an updated RFP is issued, the previous RFP will be rescinded and superseded by the updated version. Each RFP and any subsequent revisions will be identified by a revision number to provide visibility into the current version. Those interested in responding to this RFP should carefully monitor the MxD website from the original posting date through the proposal submission date for any updates or revisions

The Respondent to an RFP is the non-Federal organization that provides a submission in response to the RFP. The Respondent is considered the Prime contractor. Any other companies involved are considered Subcontractors typical of a Prime/Subcontractor relationship. All

Subcontractors are subject to flow-down clauses in the Prime contract as required by all government stipulations.

. Submission to this RFP is not a commitment for further business by either MxD or the DOW

All responses to this RFP are kept strictly confidential and are shared only with DOW authorized personnel in accordance with contractual requirements.

Due to the expedited nature of this RFP schedule, Respondents are encouraged to meet with MxD project members and ask any questions for clarification purposes. Note that responses to questions may be made public to all Respondents.

Direct all questions to both:

Patrick Barrett
Sr. Project Manager
Patrick.barrett@mxdusa.org

Emily Shanker
Mgr. System Integration, Engineering
Emily.shanker@mxdusa.org

mxdusa.org
@mxdinnovates
info@mxdusa.org

1415 N. Cherry Avenue
Chicago, IL 60642
(312) 281-6900

TECHNICAL SUMMARY



IV. TECHNICAL SUMMARY

PROBLEM STATEMENT

The Navy Organic Industrial Base (OIB) has a mix of legacy and modern equipment that lack connectivity, interoperability, and real-time visibility into operations. These constraints significantly limit the adoption of modern digital capabilities such as digital twins, Artificial Intelligence (AI), predictive maintenance, and advanced process optimization that is required for operational agility, data-driven decision-making, and can enable cybersecurity vulnerabilities.

OVERVIEW AND BACKGROUND

The NAWCAD Lakehurst Prototype and Manufacturing Division (PMD) facility has more than 305,000 square feet of industrial campus, with more than 300 computer controlled and conventional manufacturing machines. The purpose of this applied research project is to develop and demonstrate a comprehensive, cyber-secure digital manufacturing architecture for a Navy Organic Industrial Base (OIB) manufacturing facility – NAWCAD Lakehurst Prototype and Manufacturing Division (PMD). The need is driven by the necessity to modernize legacy manufacturing and maintenance operations, which currently rely on disconnected systems and manual processes. This limits operational agility, data-driven decision-making, and introduces cybersecurity vulnerabilities.

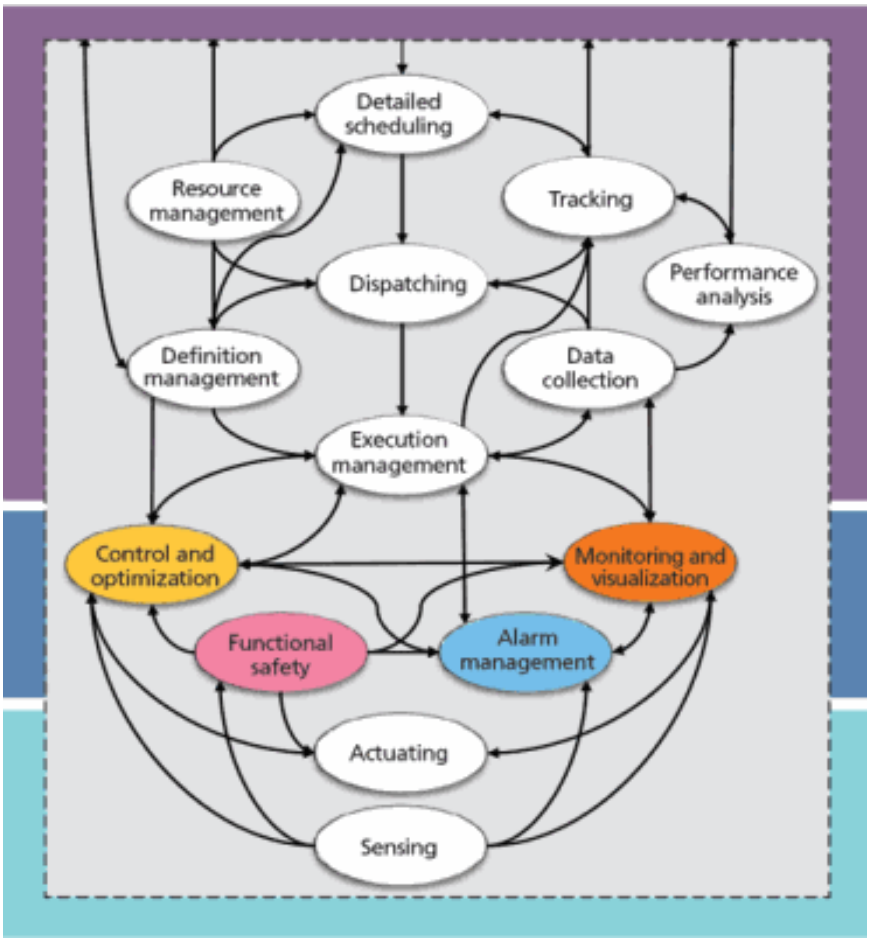
This project will address these gaps by assessing, developing, and demonstrating a standard set of processes and digital tools within a live testbed environment. This effort will validate flexible and responsive warfighter readiness solutions. The project will be executed through MxD to leverage industry best practices, foster innovation, and establish a proven, vendor-agnostic modernization blueprint that can transition to the broader Navy OIB.

OBJECTIVES

The primary objective of this project is to define a scalable Open Systems Architecture at NAWCAD Lakehurst PMD, including: Operational Technology (OT) Layer Integration, Connectivity and Network Infrastructure, Edge/Integration Layer, Data and Storage, Enterprise and Manufacturing Application Integration and Interfaces, Supplemental Analytics and Manufacturing Intelligence, and Comprehensive Cybersecurity. To demonstrate the scalability and effectiveness of the framework, use cases will be implemented as a proof-of-concept, including the connection of at least 75 pieces of equipment to the system.

The basic problem that needs to be solved is the moving data back and forth between equipment and a central location(s) in the prescribed secure manner per the use cases listed. Data availability for use at the source location (operators) is required. The goal is to improve cost, schedule, and performance for the parts delivered to the warfighter. This will be accomplished by empowering operators and managers with previously unavailable data.

The ISA-95 Activity Model shown below can be used as a reference to support the respondent in identifying the types of functionalities across Production, Maintenance, Quality, and Inventory domains which might be most valuable as a proof-of-concept within this project.



ISA-95 Extended Activity Model

REQUIREMENTS

The contractor shall execute the project through four primary phases:

1. Current State Assessment
2. Architecture Definition and Engineering Development
3. System Integration and Commissioning
4. Demonstration, Validation and Transition.

General Requirements

Throughout the project, the contractor shall:

- Work collaboratively with MxD and NAWCAD Lakehurst PMD throughout the project to ensure that the resulting architecture, technologies, and use cases align with PMD operational requirements and can be sustained and expanded by NAWCAD Lakehurst.
- Prioritize commercially available technologies and standards-based solutions where practical in alignment with the required Open Systems Architecture approach. Proposed solutions shall emphasize interoperability, scalability, maintainability, cybersecurity, and the ability to operate within the applicable NAWCAD Lakehurst IT/OT environment.
- Coordinate with NAWCAD Lakehurst IT, cybersecurity, and other appropriate stakeholders to identify applicable security requirements and ensure that the proposed

architecture and implementation support the necessary authorization and accreditation activities, including providing requested artifacts to support the ATO process.
- Address the deficiencies and mitigate the risks identified in DODIG-2021-098 and GAO-23-106576
- Meet DFARS supply chain cybersecurity rules, ITAR export regulations, and applicable CMMC standards for handling Navy technical data.
- Meet requirements for IL5 environment, processing Controlled Unclassified Information data.
- Minimize necessary equipment downtime. NAWCAD Lakehurst is a critical operating facility – all downtime must be scheduled and approved by the NAWCAD Lakehurst team.

Current State Assessment

The purpose of this phase is to establish a comprehensive understanding of the existing manufacturing, IT, OT, network, data, application, and cybersecurity environments at NAWCAD Lakehurst PMD. The assessment shall inventory all manufacturing equipment, and identify existing capabilities, limitations, gaps, and opportunities that will inform the target Open Systems Architecture and prioritization of proof-of-concept use cases (see Appendix B).

During this phase, the contractor shall:

- Prepare an assessment approach, including assessment methodology, required stakeholder participation, site activities, information requirements, and planned deliverables, for approval by MxD and NAWCAD Lakehurst PMD.
- Conduct an onsite assessment of the manufacturing facility and associated IT/OT environment.
- Develop an inventory of manufacturing equipment and relevant digital assets, documenting:
    - Equipment Identification – Equipment name, manufacturer, model, serial number, physical location, production area, etc.
    - Data Availability – What information already exists in a digital format for extraction from this equipment? Will additional sensors/logic/etc. be needed to capture relevant information?
    - Communication Availability – Does the controller/system have an existing method for natively outputting data in a modern, cybersecure manner? Is it already connected to the facility network?
    - Functional Fit – Is there missing or underdeveloped operational functionality that could be addressed within this project? What problems do teams face today with this piece of equipment which could be solved with data?
- Submit the completed “Use Case Feasibility And Equipment Mapping” matrix (see Appendix A) for the identified use cases and inventoried equipment to aid NAWCAD Lakehurst and MxD in the final selection process for proof-of-concept implementation.

Phase Completion Milestone: The Current State Assessment shall culminate in a Current State Assessment Report that documents the existing environment, identified gaps and opportunities, equipment and data inventory, current-state architecture, and recommended priorities for subsequent phases.

Architecture Definition and Engineering Development

The purpose of this phase is to translate the findings of the Current State Assessment into a scalable target Open Systems Architecture and develop the detailed engineering definition necessary to implement the initial proof-of-concept. The target architecture shall establish a reusable framework that can support additional equipment, use cases, data sources, applications, and manufacturing sites beyond the initial project implementation.

During this phase, the contractor shall:

- Develop and document the target Open Systems Architecture, including, at a minimum:
  - Operational Technology (OT) layer integration
  - Connectivity and network infrastructure
  - Edge computing and integration layer
  - Data collection and ingestion, including required communication protocols (ex. MTConnect)
  - Data storage (if design exceeds 20TB planned usage) and historian capabilities
  - Enterprise and manufacturing application integration
  - Applications and user interfaces
  - Analytics and manufacturing intelligence
  - Identity, access control, and cybersecurity
- Define cybersecurity requirements and architecture, including applicable security boundaries, authentication and authorization, account management, encryption, logging, monitoring, vulnerability management, and other controls necessary to support the target environment and NAWCAD Lakehurst's authorization and accreditation process (see Appendix C).
- Define functional and technical requirements and develop detailed engineering designs and implementation plans for the proposed use cases, for approval by MxD and NAWCAD Lakehurst PMD.
- Define the Plant Model of the facility to automate real-time tracking of Overall Equipment Effectiveness (OEE), machine downtime, and scrap rates.
- Define a robust, secure, and flexible API architecture using open data standards (e.g. JSON, .xml, .yaml) to facilitate the seamless integration of downstream Navy systems. The API shall support on-demand data queries and event-based broadcasting. This can be achieved either by bulk data synchronization or live querying. This ensures Navy systems can either replicate the data locally or visualize it in real time without duplicating storage. To maintain a secure interface, the performer shall utilize FIPS 140-3 approved cryptographic methods, public key infrastructure (PKI) authentication, and enforce role-based access, ensuring user credentials and permissions seamlessly pass through the integration.
- Define a data governance framework for the target architecture for review and approval by MxD and NAWCAD Lakehurst PMD.
- Develop a procurement plan and bill of materials for required hardware, software, licenses, services, and other implementation materials.

- Identify long-term scalability requirements and establish a roadmap for expanding the architecture beyond the initial proof-of-concept.

Phase Completion Milestone: The Architecture Definition and Engineering Development phase shall result in an approved Target Open Systems Architecture and sufficient engineering definition to proceed with implementation without requiring fundamental redesign of the solution.

System Integration and Commissioning

The purpose of this phase is to implement and integrate the approved Open Systems Architecture and proof-of-concept capabilities within the NAWCAD Lakehurst PMD environment. The contractor shall coordinate closely with NAWCAD Lakehurst personnel to ensure that installation and configuration activities comply with applicable facility, IT, OT, cybersecurity, safety, and operational requirements. MxD will support coordination as necessary.

During this phase, the contractor shall:

- Procure and receive required hardware, software, licenses, networking equipment, sensors, edge devices, and other implementation materials.
- Implement the selected proof-of-concept use cases and Plant Model.
- Install physical and digital infrastructure and equipment required to implement the target architecture onsite at NAWCAD Lakehurst
- Commission the integrated system and demonstrate that the implemented capabilities operate as intended within the NAWCAD Lakehurst environment.
- Perform equipment-level and subsystem-level integration testing on the 75+ selected machines prior to full system validation.
- Document the final installed configuration, including equipment connectivity, network configuration, software configuration, data flows, interfaces, and cybersecurity controls.
- Update the target architecture and engineering documentation to reflect any approved changes made during implementation.

Phase Completion Milestone: The System Integration and Commissioning phase shall result in the target Open System Architecture with specified use cases implemented at NAWCAD Lakehurst which are ready to proceed through verification and validation testing.

Demonstration, Validation and Transition

The purpose of this phase is to demonstrate that the implemented Open Systems Architecture and proof-of-concept capabilities satisfy the approved requirements, establish operational acceptance, and transition the system and associated knowledge to NAWCAD Lakehurst PMD personnel.

During this phase, the contractor shall:

- Develop a detailed System Verification and Validation Plan defining:
- Conduct Factory Acceptance Testing (FAT), where applicable, prior to deployment or final commissioning.
- Conduct Site Acceptance Testing (SAT) following installation and integration at NAWCAD Lakehurst.

- Perform cybersecurity testing and validation appropriate to the implemented architecture and in coordination with NAWCAD Lakehurst cybersecurity personnel.
- Support cybersecurity authorization activities, including preparation and delivery of required technical documentation, system descriptions, architecture diagrams, configuration information, security control evidence, and other documentation required to support the applicable Authority to Operate (ATO) process.
- Develop and deliver final system documentation.
- Develop and conduct training for NAWCAD Lakehurst personnel responsible for operating, administering, maintaining, and expanding the digital manufacturing environment.
- Provide a defined period of post-commissioning technical support to address defects, configuration issues, and other implementation-related issues identified during initial operational use.
- Provide warranty and/or maintenance support for procured hardware and software in accordance with applicable manufacturer or supplier terms.

Phase Completion Milestone: The Demonstration, Validation and Transition phase shall result in the contractor demonstrating that the implemented solution meets the approved requirements and acceptance criteria and has transitioned the system, documentation, and operational knowledge to NAWCAD Lakehurst PMD. Critical project completion KPIs are listed below:

1. >75 machines within NAWCAD Lakehurst PMD connected to delivered solution
2. >50 connected machines have actionable information available to the operator directly at the machine

Roles and Responsibilities (RACI)

(R=Responsible; A=Accountable; C=Consulted; I=Informed)

Project Task	MxD	NAWCAD Lakehurst	Sub-recipient(s)
Overall Project Management & OTA Admin	A	C	R
Define OIB Requirements & Use Cases	C	A	R
On-Site Asset Discovery & Access	C	A	R
On-Site Coordination & Access	C	R	C
Design OT Network & Plant Model	C	A/C	R
Procure Hardware/Software	I	C	R/A
Install Hardware	I	C	R/A
Install Software	I	R	C
System Integration & Testing	C	R/I	R/A
Submit & Manage RMF/ATO Package	I	R/A	C
Final Blueprint & Report Authorship	C	A	R

Out of Scope

There are significant unknowns that could impact the project due to the complex nature of the existing manufacturing, IT, OT, network, data, application, and cybersecurity environments at

NAWCAD Lakehurst PMD. The following list outlines specific tasks that are out of scope for this project such as:

- Interim Authority to Test (IATT) Processing, this task would be led by the government team
- Authority to Operate (ATO) Approval, final ATO approval authority and decision resides with NAWCAD, not the performer

mxdusa.org
@mxdinnovates
info@uilabs.org

1415 N. Cherry Avenue
Chicago, IL 60642
(312) 281-6900

PROGRAM OVERVIEW

V. PROGRAM REQUIREMENTS

PROGRAM MANAGEMENT

The selected Respondent will be awarded a contract as the Awardee. The Awardee is responsible for managing the project to ensure the team meets all the technical objectives and requirements as contracted based on the proposal.

FUNDING REQUIREMENTS

MxD anticipates awarding a fixed-price contract resulting from this RFP.

Cost share is not required for this contract. However, cost share is encouraged to support the Institute's mission

The total funding available for this project shall not exceed $2,700,000 of Federal Funding, not inclusive of optional cost share. Respondents must submit a cost proposal outlining the cost associated with their proposed solutions. While the format of the proposal is flexible, the following information must be clearly included:

1) Summary of background experience demonstrating domain qualifications and expertise
2) Experience level and number of headcount being proposed for this effort
3) Acknowledgement that all headcount are US citizens subject to a criminal background check (see note below)
4) Hourly rate for proposed headcount
5) Total hours proposed for the project
6) Total cost (see note below)

Neither MxD nor the U.S. Government has any responsibility for costs associated with development, submissions, or pre-award negotiations for this proposal and subsequent contracts.

TRAVEL, FACILITY ACCESS AND INSURANCE REQUIREMENTS

All travel requirements and associated costs needed for execution of the objectives and deliverables must be included in the proposal. There is no increase in funding should additional travel be required to fulfill the agreed upon requirements

PERIOD OF PERFORMANCE REQUIREMENTS

Estimated period of performance (Execution PoP) is 24 months from contract award execution and project must be completed no later than May 2029.

OWNERSHIP OF DELIVERABLES AND INTELLECTUAL PROPERTY

Background IP, meaning intellectual property that was developed outside this project or existed before it, remains solely owned by the Contractor. Where Background IP is incorporated into, or is necessary to use, maintain, or extend a deliverable or any Project IP, the Contractor will grant the USG a license sufficient to enable that use. Background IP that will be incorporated into a deliverable will be identified to the Government in advance.

Intellectual property developed specifically for and in the performance of this project ("Project IP") will be owned by the United States Government (USG). The specific rights, licenses, and materials provided to the USG will be tailored to the nature and intended use of each deliverable, as described below.

- **The OIB Modernization Blueprint:** The final blueprint document, including all process descriptions, architectural diagrams, research findings, and lessons learned, will be delivered with Unlimited Rights, allowing free distribution and use across the entire DoW and its support contractors.
- **Project-Developed Software:** Any new software code developed specifically for this project (e.g., data normalization shims, custom dashboards) will be delivered with Government Purpose Rights (GPR), or other rights as tailored to the deliverable.
- **Project Data:** All configuration files, asset inventories, and performance data generated by the project will be delivered with Government Purpose Rights (GPR), or other rights as tailored to the deliverable.

The specific rights, licenses, and materials provided to the USG, including any license to Background IP, will be sufficient to enable the Government to operate, maintain, modify, integrate, replace, and further develop the applicable deliverables, including through third parties where appropriate. Such rights will support the Government's open architecture objectives.

VI. ELIGIBILITY

MxD Membership

This RFP is open to the public; any organizations regardless of membership status may submit a proposal in response to this RFP. However, once a Proposal Team is downselected, each member of the Proposal Team shall execute the **MxD Membership Agreement and Standard Project Agreement (SPA)** within 30 days of notification of project downselect; acknowledgment of this is required in the Technical Proposal submission.

Any non-MxD members are strongly encouraged to conduct a legal pre-review of the Membership Agreement and Standard Project Agreement (SPA) before submission, as this is a common source of delay during negotiations with proposal teams chosen during downselection.

Proposals submitted by active MxD members shall ensure they are in good standing and have an executed Standard Project Agreement (SPA) within 30 days of notification of project downselection. If an active MxD member has not executed the SPA, they are strongly encouraged to execute the SPA as early as proposal submission, as this is a common source of delay during negotiations with proposal teams chosen during downselection

For information on MxD membership, including pricing and benefits, please contact MxD's Business Development Manager, Chad Crump (chad.crump@mxdusa.org). For more information on becoming a MxD Member, please visit the MxD Membership page on our website. Federally Funded Research and Development Centers (FFRDCs) and Government entities (Government/National laboratories, military educational institutions, etc.) are subject to applicable direct competition limitations. They cannot propose Project Calls in any capacity unless they address the following conditions:

- FFRDCs or Government entities may not exclusively team on any specific proposal team.
- FFRDCs must demonstrate that the proposed work is not otherwise available from the private sector and must also provide a letter on letterhead from their sponsoring

organization citing the specific authority establishing their eligibility to compete with industry and propose to solicitations utilizing Government funding.

- Government entities must clearly demonstrate that the work is not otherwise available from the private sector and provide written documentation citing the specific statutory authority and, where relevant, contractual authority, establishing their ability to propose to solicitations utilizing government funding.

Government agencies interested in participating in MxD RFPs as a respondent or subcontractor should notify MxD in advance of the RFP submission. For RFPs utilizing federal funding, special agreements and considerations may need to be implemented to enable participation.

Notification of Participation Non-U.S. Citizens

Award shall be granted only to U.S. companies, firms, organizations, institutions, or other entities organized or existing under the laws of the United States, its territories, or possessions (as defined in Section 120.15 of International Traffic in Arms Regulations, 22 CFR § 120 et. seq. ("ITAR")).

It is a requirement that work related to the Award must be completed in the U.S. by people legally authorized to work in the U.S.

VII. PROPOSAL EVALUATION

Evaluation Process for Project Calls

An MxD Evaluation Board (EB) will review and evaluate each submitted proposal using the evaluation criteria noted below.

Evaluation Criteria

Each proposal is evaluated by a specific set of criteria. Below are the proposal evaluation criteria for this RFP:

Proposal Evaluation Criteria
Requirements Compliance • *Proposed solution clearly addresses all mandatory objectives identified in RFP* • *Clear identification of assumptions, risks, and mitigations* • *Complete and clear itemization of all requirements* • *Program management plan meets requirements in the RFP*
Respondent Qualifications • *Respondent is highly qualified to accomplish the tasks with clear delineation of roles and responsibilities* • *Respondent has unique capabilities that are directly associated with the target technology and tasks* • *Proposed project work participants are in compliance with restrictions on foreign firms and/or non -US Citizens*

Cost Factors Requirements

- *Proposed cost estimates are reasonable and realistic for the proposed work effort*
- *Value is maximized through inclusion of optional cost share and objectives*

SUBMISSION DETAILS

Each Respondent must submit their proposal no later than 5:00PM Central Time, November, 13, 2026. All submissions must be submitted electronically to MxD's submission form, LINK HERE. **Please complete the form and hit SUBMIT in order to fully submit your proposal.**

Notice of Intent to Submit: If you plan to respond to this RFP please notify the Project Contact via email by November 09, 2026. This expression of interest helps the project team effectively manage the evaluation timeline

VIII. NEXT STEPS

NOTIFICATION

MxD will notify all Respondents of the status of their proposal by December 07, 2026. This notification will include decision of the EB. If the proposal has been accepted for award, instructions for next steps will be reviewed with the selected Respondent.

FINAL REVISIONS

MxD reserves the right to negotiate the cost and scope of the proposed work with a Respondent that has been down selected. The selected Respondent(s) and subcontractors, if any, who intend to pursue selection may be required to participate in the revision process prior to award.

CONTRACT

Final contract vehicle and contract terms will be negotiated at the time of contracting. Down selection of a proposal does not constitute agreement to quoted terms by either MxD or the DoW.

I. APPENDIX A

USE CASE FEASIBILITY AND EQUIPMENT MAPPING MATRIX

Create a Use Case Feasibility and Equipment Mapping Matrix that helps a broad audience quickly grasp why this modernization effort is so sprawling and complex. The matrix should reveal two key dimensions simultaneously: the wide spectrum of equipment digital readiness — ranging from legacy standalone systems to networked modern machines — and the project's cross-cutting scope across multiple manufacturing domains (Production, Maintenance, Quality, and Inventory). By making both visible and countable, the matrix will enable Lakehurst to identify which use-case-to-equipment combinations are technically achievable given current readiness, and which offer sufficient value to justify the investment.

The attached sample matrix is for illustration purposes only, it is intended solely to convey the conceptual structure and was created with assistance from artificial intelligence. The Contractor is responsible for designing and populating the final matrix with authoritative, operationally validated information.

Use Case Feasibility and Equipment Mapping Matrix — Sample Illustration

Shows how equipment readiness (legacy to modern) maps to use cases across four manufacturing domains

Equipment & Readiness				Use Case (Production Domain)				Feasibility & Mapping			
Equipment ID	Type/Age	Data Availability	Network Ready	Use Case	Domain	Business Value	Technical Complexity	Feasibility	Data Gaps	Readiness Investment	Counts Toward 75?
Mill-03	Legacy (1995)	No — manual logsheets only	No	Real-time production tracking	Production	High	High — needs sensors + gateway	Challenging	Vibration, temperature, cycle time	Edge gateway + 3 sensors	Yes
CNC-07	Semi-Modern (2008)	Partial — controller outputs spindle load only	No — isolated network	Predictive maintenance	Production	High	Medium — needs connectivity + analytics	Moderate	Vibration, bearing temp; network connection	Network drop + vibration sensor	Yes
Mill-12	Modern (2020)	Yes — OPC-UA native output	Yes — networked	OEE dashboard + real-time alerts	Production	Medium	Low — mostly configuration	Feasible	None (full data stream available)	Configuration + analytics software	Yes
Welder-02	Legacy (1998)	No — manual maintenance logs only	No	Maintenance scheduling optimization	Maintenance	High	High — retrofit needed	Challenging	Duty cycle, consumables usage, failures	Sensors + edge device + analytics	Yes
Inspect-04	Semi-Modern (2012)	Partial — CMM outputs to USB only	No	Quality record centralization	Quality	Medium	Medium — needs network + integration	Moderate	Integration to MES; historical data archive	Network connection + integration adapter	No

Color legend:

- Red tint: Legacy systems (pre-2000s)
- Green tint: Modern systems (post-2015)
- Green feasibility: Fully achievable with current/minor investment
- Yellow feasibility: Partial — moderate readiness investment needed
- Red feasibility: Challenging — significant retrofit/integration required

Notes: This sample shows 5 machines across 3 domains (Production, Maintenance, Quality). A full matrix would show all 300+ inventoried equipment, all candidate use cases, and all four domains (Production, Maintenance, Quality, Inventory). The matrix helps prioritize which use-case-to-equipment combinations offer the highest return on readiness investment.

II. APPENDIX B

USE CASE EXAMPLES (INFORMATION PURPOSES ONLY)

The scope of this effort requires the selected performer to collaborate with the Navy to identify pain points and develop tailored solutions. The use cases detailed below are a representative sample of scenarios, intended to provide performers with upfront insight into the objective end-state capabilities.

Data Driven Programming (Before)

Focus Area: Providing operators with historical part-family data, approved models, and tribal knowledge before programming to minimize NRE and reduce scrap rates.

Use Cases:

1. Establishing a single, version-controlled repository to ensure machinists always have access to the correct 3D models and G-code, eliminating redundant reprogramming.
2. Automatically provide proven speeds, feeds, and tooling selections from geometrically similar "part/feature families" during the programming.
3. Digitizing machinist setup notes, fixture details, and operator tips so they are instantly searchable and linked to the part number.
4. Provide a real time machine capability matrix to allow machining operations (machine selection) to be optimized based on capability.

Active Process Monitoring (During)

Focus Area: Instrumenting critical assets with sensors to monitor and correct the machining process in real time.

Use Cases:

1. Generating real-time, on-screen alerts for operators when a process variable (such as coolant flow, pressure, or spindle speed) deviates from the operating baseline.
2. Tracking sensor trends across a production run to identify when a process is drifting out of control before dimensional tolerances are exceeded.
3. Monitoring for sudden spikes in sensor data to detect imminent damage to the part from issues like tool wear, triggering an automated pause to save the part.

Adaptive Quality Feedback (After)

Focus Area: Correlating digital inspection data with machine parameters to drive advanced analytics and continuous process improvement.

Use Cases:

1. Correlating post-process quality data with machine history and parameters to determine what impacted part accuracy.
2. Using digital inspection data from completed parts to automatically calculate and feed tool-offset adjustments back to the CNC controller for subsequent runs.
3. Feeding post-process analytics (such as optimal speeds, feeds, and tooling performance) back into the Pillar 1 repository for future programming.

Operational Metrics (OEE)

Focus Area: Adapting OEE metrics to a high-mix, low-volume environment to provide high value operational metrics.

Use Cases:

1. Providing real-time dashboards showing true machine availability, first-pass quality, and schedule adherence to give a comprehensive overview of shop performance.
2. Monitor critical assets to identify mechanical wear and schedule maintenance before an unplanned outage occurs.
3. Automatically separate NRE activities—such as programming, setup, and first-article validation—from active machining time to accurately analyze process bottlenecks and true machine utilization.
4. Provide optimized scheduling recommendations based on machine usage and the trade space for machine capabilities (Pillar 1)

III. APPENDIX C

OT CONTROLS

The following lists identify the minimum cybersecurity requirements for the delivered solution where it connects to Operational Technology (OT) systems. The solution shall not introduce, or rely on, any of the conditions below. Failure to implement the listed security controls, or the presence of any listed unsupported component or prohibited port or protocol, will prevent the solution from receiving authorization to connect to the target environment.

The requirements fall into three categories:

1. Required Security Controls – Controls from NIST SP800-3 that must be implemented and demonstrable for all connected OT systems
2. Unsupported and Prohibited Hardware and Software – Components that are end-of-support, carry known critical vulnerabilities, or are prohibited by directive.
3. Ports, Protocols, and Services Management (PPSM) – Network ports and protocols that shall not be used.

Disqualifying controls/findings for connected Operation Technology (OT) systems

- CM-8 — System Component Inventory
- CA-3 — Information Exchange
- AC-3 — Access Enforcement
- AC-6 — Least Privilege
- AC-17 — Remote Access
- IA-2 / IA-3 / IA-5 — User/device authentication and authenticator management
- SC-7 and SC-7(5) — Boundary Protection and Deny-by-Default/Allow-by-Exception
- AU-2 / AU-6 / AU-12 — Event logging, review, and generation
- SI-4 — System Monitoring
- CA-7 — Continuous Monitoring
- CM-6 — Configuration Settings
- IR-4 — Incident Handling
- SC-12 / SC-13 — Cryptographic Key Management and Cryptographic Protection

Unsupported SW/HW

- SA-22a (Rev 5) - Unsupported System Components (HW/SW)
- Legacy / Vulnerable (<2.17) Log4j (High vis for NAO)
- Anthropic Products (banned per EXORD)

PPSM

- Telnet Port 23
- FTP Port 20,21

IV. APPENDIX D

CONTROL SYSTEM/OT SECURITY ARCHITECTURE

The scope of this effort requires the selected performer to work within Levels 0, 1, and 2 of the reference architecture below (Figure 2). Connection points to Level 3 and above will be provided by NAWCAD Lakehurst.

Reference:

DoW CONTROL SYSTEMS/ OPERATIONAL TECHNOLOGY SECURITY REQUIREMENTS GUIDE,

27 February 2026, Version 2, cleared for Open Publication Apr 28, 2026

The reference architecture below (Figure 2) is the 5-level Control System/OT Architecture, used in UFC 4-010-06, Cybersecurity of Facility-Related Control Systems. This architecture is defined as a general architecture suitable for a wide range of control systems/OT. For many Departments control systems/OT the 5L- Control systems/OT reference architecture is a key tool for understanding the layering aspect of control system/OT security architecture and IP/non-IP delineation; however, this architecture may not be a useful representation for all control system/OT environments. Given the diversity of control systems/OT in their complexity and capabilities, this architecture will not apply to all DoW control systems/OT. Rather, the architecture can be used to understand key security architecture concepts that may benefit system owners when securing their control system/OT environments. reate a Use Case Feasibility and Equipment Mapping Matrix that helps a broad audience quickly grasp why this modernization

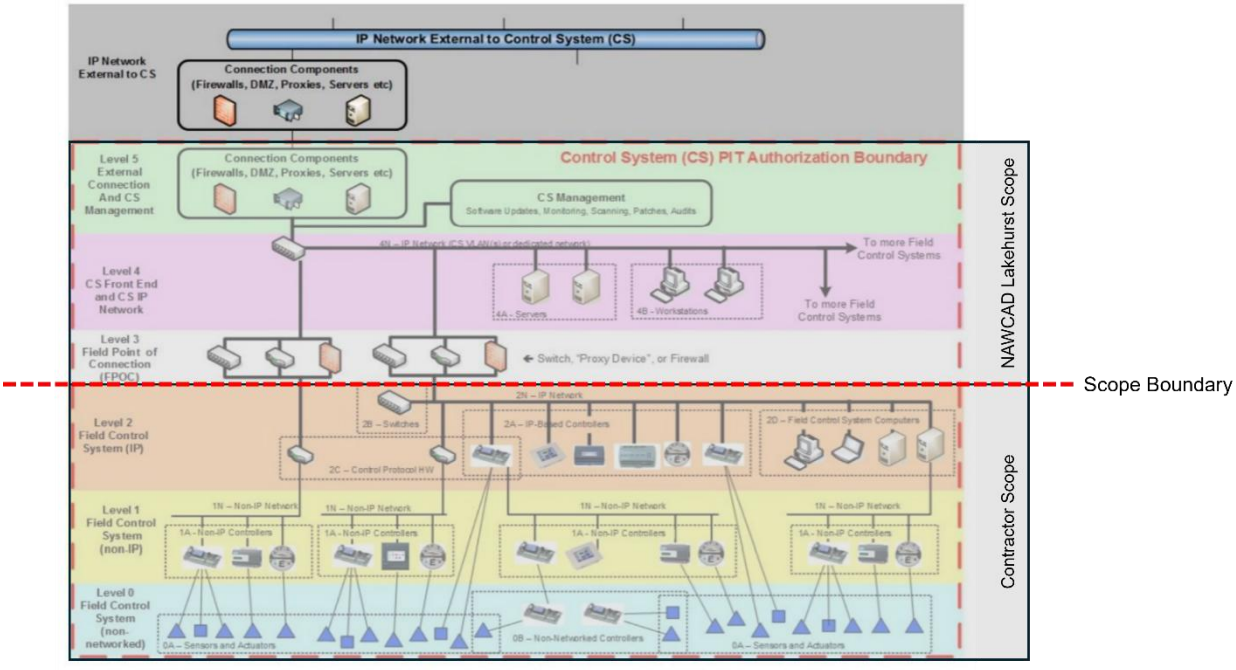


Figure 2: UFC-4-101-06 (5-Level Control System/OT Architecture)