The Digital Manufacturing Institute

MxD REQUEST FOR PROPOSAL

TECHNICAL SUMMARY, PROGRAM OVERVIEW and PROPOSAL PREPARATION INFORMATION

MxD-21-11:

Security Solutions for OT Factory Equipment

Revision 1.0 Release Date: September 20, 2021

Contact: Scott Kruse
Project Engineer
MxD
projects@mxdusa.org

MxD
1415 North Cherry Ave
Chicago, IL 60642

TABLE OF CONTENTS

I. RECORD OF CHANGE

Revision	Date	Sections	Description
1.0	20 September, 2021	N/A	Original

II. PROJECT OVERVIEW

RFP Released	20 September, 2021
Pitch Session (Optional)	13 October, 2021
Technical and Cost Proposal Due	18 November, 2021
Anticipated MxD Funding	$500,000
Period of Performance	12 Months

III. INTRODUCTION

MxD: The Digital Manufacturing Institute is where innovative manufacturers go to forge their futures. In partnership with the Department of Defense, MxD (also referred to as the Institute) equips U.S. factories with the digital tools and expertise they need to begin building every part better than the last. MxD's core mission is to transform American manufacturing, by fully integrating the digital thread across the manufacturing enterprise to reduce overall manufacturing costs, stabilize and grow the manufacturing industrial base and improve US competitiveness through the world.

MxD has invested over $120 million in more than 85 applied research and development projects in areas including design, product development, systems engineering, future factories, agile and resilient supply chains, and cybersecurity.

MxD operates from a nearly 75,000-square-foot innovation center near downtown Chicago. Its future factory floor features some of the most advanced manufacturing equipment in the world, which partners can use for experimentation and training on everything from augmented reality to advanced simulation techniques.

MxD uses a broad and collaborative process to develop the Strategic Investment Plan (SIP) and Technology Roadmap to ensure its technology, outreach, and education investments provide U.S. manufacturing with the right skills, solutions, and tools to compete globally. A Request for Proposal (RFP) is initiated when MxD desires new and creative solutions to problems and/or advances in knowledge, understanding and technology for digital manufacturing and design. Once the RFP topic is developed and approved, the MxD RFP will be posted to the MxD website and represents the official notification to Proposal Teams of a request to submit the required documents.

This RFP contains the following elements:

1. Technical Summary: description of a specific technology objective
2. Program Overview: description of technical and program requirements

3. Proposal Preparation Information: background and guidance for the preparation of required forms and instructions needed to submit a proposal to MxD

The RFP is available on the MxD website at https://mxdusa.org/projects/. Amendments to a 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. Proposal Teams should carefully monitor the MxD website after an original posting of an RFP, up to the time of the Technical Proposal and Cost Proposal submission date. Any revisions, amendments or updates will appear in the same section of the website as the original solicitation. It is the responsibility of the Proposal Team to monitor the MxD RFP updates and ensure their proposal meets the solicitation requirements. MxD welcomes any comments or suggestions for improving the contents of this guide. Please address them to projects@mxdusa.org.

MxD refers to the Proposal Team Lead as the non-Federal organization that submits a proposal in response to a Request for Proposals. Proposal Team members are other participants on the proposal and are further broken down into Recipient/Subrecipient relationships similar to a prime/subcontractor relationship in traditional contracting.

Any questions regarding this solicitation must be provided to projects@mxdusa.org. The questions will be sent to the appropriate MxD and/or Government POC, and answers will be published on the MxD website, if appropriate. Questions submitted within one week prior to a deadline may not be answered.

mxdusa.org
@mxdinnovates
info@mxdusa.org

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

TECHNICAL SUMMARY

mxdusa.org
@mxdinnovates
info@mxdusa.org

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

IV. TECHNICAL SUMMARY

PROBLEM STATEMENT

Manufacturing operations are becoming increasingly digital and internet connected, this introduces security concerns for Operational Technology used in manufacturing facilities. The traditional cybersecurity approach for an Operational Technology (OT) manufacturing environment is air-gapping or network segmentation to keep it separate from the Informational Technology (IT) environment. In today's context of Industry 4.0, this traditional approach is prohibitive in driving maximum value from digital manufacturing implementations. With a growing number of solutions available for manufacturers to leverage shop floor data and increase operational efficiency, a connected factory floor with networked OT equipment joining IT ecosystems is quickly becoming a necessity to remain competitive in American manufacturing. The blending of OT equipment and IT systems is creating a new set of security concerns for manufacturers to consider in their operations. Manufacturers must leverage data from legacy equipment along with new equipment to gain the most value from digital manufacturing solutions while ensuring that they do not expose critical data to malicious outside parties. The cyber threat landscape for OT equipment controlling production operations has grown rapidly along with the growing ecosystem of digital technologies in the manufacturing sector.

Despite the threat of cyber-attacks hanging over the manufacturing industry, the adoption of cybersecurity solutions and proper cyber hygiene for manufacturing OT equipment is lagging. Taking a closer look at why cybersecurity initiatives are falling short in the manufacturing sector, MxD identified an opportunity to advance adoption of proper cybersecurity practices for manufacturers. Cybersecurity solution providers have existed for a long time to serve the IT ecosystem and these traditional security controls help in the OT environment along with the quickly growing OT specific cybersecurity solution space. It is not due to a lack of available cybersecurity tools that is holding manufacturers back from securing their OT environments. In an industry where operational efficiency and production throughput are the main focus, cybersecurity is viewed as an afterthought or a "nice-to-have" rather than a "must have" for manufacturers. The potential cost of cyber threats is not often considered when budgeting for OT cybersecurity and the return on investment (ROI) for cybersecurity implementations is not prioritized. Manufacturers are susceptible to costly cyber threats, whether it is a ransomware attack that shuts down operations, a data breach exposing trade secrets, or a targeted attack on OT equipment that halts production.

Another hurdle the manufacturing sector faces in OT cybersecurity is a lack of resources. Most small to medium size manufacturers (SMMs) lack IT and cybersecurity personnel who may not understand the cyber threats and how to prepare for a connected shop floor. While larger manufacturing organizations may have a more sophisticated cybersecurity posture, the manufacturing sector is overwhelmingly made up of small and medium sized organizations. SMMs are uncertain how to kick-off their cybersecurity journey which includes identifying essential cybersecurity solutions and implementing these tools effectively in their operations. It is a lack of cybersecurity expertise and understanding that leads to poor OT security from cyber threats throughout the industry. Making cybersecurity tools available to keep OT environments secure without interrupting operations is a key need in the manufacturing industry.

MxD is funding a project to help accelerate the adoption of cybersecurity solutions in the OT environment. This effort will address the perceived hurdles that small and medium sized manufacturers face in cybersecurity as discussed above. Through this investment, MxD seeks to create a set of tools that enable manufacturers of all sizes to understand the business case for cybersecurity in their OT operations and a user-friendly playbook or framework that illustrates the steps to securing OT equipment in a manufacturing environment. Because most manufacturers do not have cybersecurity expertise, it is important that the outcome of this project is geared to be user-friendly and easy to understand. A successful proposal will explore and verify the hurdles identified by MxD, prove ROI of OT cybersecurity to SMMs, develop a tactical roadmap or playbook, and demonstrate a successful implementation of this playbook at the MxD Factory Floor environment.

OBJECTIVES

The following objectives outline the key activities that MxD considers applicable for a successful project. MxD's recommended set of requirements are included under each objective, but the team is encouraged to make value-added changes to the requirements as they see fit. These changes should be justified in their proposal. The objectives below are listed in a rough chronological order based on a general concept of project execution but accomplishing tasks in this specific order is not a requirement. MxD encourages agile development on its projects to ensure that the deliverables are shaped and validated by customers and key stakeholders throughout the period of performance.

Because the objectives are listed chronologically, they are not listed in order of importance to MxD. Teams are encouraged to maximize the impact of MxD funding by targeting research areas where team members have performed prior work, already possess components of the end solution, or where prior MxD research can be leveraged.

The key objectives are defined below:

1. **Explore most significant pain points in OT Cybersecurity implementations:** To remain grounded in the real-world problems of manufacturers, the project should have a discovery phase to verify the pain points and barriers to success in OT cybersecurity implementations within manufacturing environments.

   In reviewing the current landscape of OT cybersecurity in the manufacturing sector, MxD identified the hurdles discussed in the Problem Statement. Those hurdles include a lack of prioritization and misunderstood ROI for cybersecurity implementations along with a shortage of expertise and knowledge in the manufacturing sector. The project team should have a discovery phase to verify our assumptions and build a more complete picture of the pain points leading to lagging or failed cybersecurity implementations. This objective seeks to address the question: "Why is it not happening?".

   The requirements for this objective are as follows:

   - Project team should target manufacturing OT environments where sufficient data is available to evaluate current cyber posture in comparison to cybersecurity goals
   - Identify which manufacturing OT environments are to be investigated and explain why they were selected along with any assumptions or constraints of the case study

- Determine criteria for prioritizing and identifying causes for gaps in cyber security and develop a plan for how the investigation will be done at the targeted manufacturers
- Project team should reference current cybersecurity standards such as NIST 800-171 and CMMC among others
- Evaluate current or previous OT cybersecurity initiatives for their success and shortcomings
- Develop a set of quantitative or qualitative metrics to report on for manufacturer's pain points in OT cybersecurity implementations
- Report findings from the discovery phase via technical report along with creating webinar content for sharing with MxD community (i.e. slides and talking points)
- The findings of this discovery phase should be shaped to further refine the team's approach to the rest of the project objectives

2. **Proving ROI of OT Cybersecurity for SMMs:** The project should develop the return on investment (ROI) for implementing OT security tools for the purpose of creating more incentives for manufacturers to adopt cybersecurity in their operations.

   Shifting the mindset from cybersecurity tools being an afterthought to being a must-have in OT environments. The project should develop the business case for implementing proper cyber practices through the costs associated with cyber risks in manufacturing operations. This objective seeks to address the question: "Why does it need to happen?"

   The requirements for this objective are as follows:

   - Identify which manufacturing OT environment(s) are to be studied for ROI and explain why they were selected along with any assumptions or constraints of the case study
   - Develop methodology and supporting framework for evaluating the return on investment for an OT cybersecurity implementation at a manufacturing facility
   - Develop a framework or template that can be used to understand the estimated costs and returns associated with different cybersecurity investments for the high value opportunity/problem areas. While exact ROI is impossible to predict, there needs to be upfront confidence that cybersecurity implementations will provide value to manufacturing operations. The impact to the bottom line must be clear
   - Project team should consider the return on investment not only as a function of cyber vulnerabilities removed, but also the operational revenue that is tied to the risk reduction accomplished through a cybersecurity implementation
   - Provide guidance on questions which need to be asked to properly benchmark cybersecurity costs and assess prospective returns of implemented solutions
   - Project team should leverage existing work where possible and take into account the current industry cybersecurity compliance standards
   - Build framework that can be applied to a broader manufacturing audience beyond the manufacturer(s) and processes being investigated by the project team
   - Optionally, the team can create a simple software tool (i.e. an excel workbook) for manufacturers to evaluate the ROI of cybersecurity in their own operations

3. **OT Cybersecurity playbook for SMMs:** The project should develop a step-by-step playbook which will serve as a simplified framework for how to achieve proper cybersecurity measures on a connected manufacturing floor.

   Building off existing solutions in the cybersecurity space, the project should explain the process of securing a factory environment from cyber threats while taking into account the pain points and barriers identified in the first objective. This must be conveyed in a broadly applicable and easily understood "playbook" that SMMs can learn from and apply in their own environment regardless of solution provider selection. This objective seeks to address the question: "How can I do it in my operations?"

   The requirements for this objective are as follows:

   - The playbook should describe the steps necessary for manufacturers to secure their operations against cyber threats while addressing the most common hurdles to cybersecurity implementations as identified in the discovery phase and highlighting the high-value ROI opportunities
   - Project team to address a wide range of starting points for cybersecurity posture, whether a manufacturing organization is starting with a blank slate or if an organization has some cyber tools in place
   - Include details of all assumptions and constraints that manufacturers must consider as they approach a cybersecurity implementation in their own environment
   - Technical report of the system infrastructure and integration framework. Including the detailed step-by-step approach and network diagrams
   - User-friendly version of a framework with guidance on the steps necessary to develop a proper cybersecurity implementation in an OT manufacturing environment
   - The playbook should include considerations for the sustained support for cybersecurity solutions beyond the initial implementation process
   - Optionally, this objective outcome could include webinar content to help reach a broader audience (i.e. slides and talking points)

4. **MxD Factory Floor implementation of the playbook:** As a hands-on demonstration of the project outcomes, the team will implement the steps identified in the cybersecurity playbook in the MxD Factory Floor OT environment.

   This is expected to be a narrative based walkthrough which explains each step in the process, how the solutions are implemented, and how they work in combination to secure an OT environment. The MxD factory floor implementation will serve as an OT Cybersecurity training and awareness resource for the MxD community and visitors to the facility. This objective seeks to address the question: "What does it look like in practice?"

   The requirements for this objective are as follows:

   - Technical report of the system infrastructure and integration framework for the MxD implementation
   - Detailed BOM (Bill of Material) that includes hardware and software specifications

- Validate proof of concept of system design and BOM by implementing and validating the system
- Install and begin final preparation for demonstration at MxD factory floor
- Technical report detailing implementation process. Story-telling based narrative presentation of this implementation process to demonstrate on the MxD Factory Floor
- Document detailing the hand-off to MxD Cyber team, MxD IT, and MxD engineering team. Include support details and ongoing costs such as licensing fees

Through these objectives, the project principally seeks to address the following use cases among other value-added use cases identified throughout the project:

- "As a plant manager with a medium sized manufacturer with networked equipment and a machine monitoring solution, our operations have vastly improved. Recent news articles on OT focused Cyber-attacks have me worried for the first time that we are not prepared. I have never been able to justify the cost and do not have any internal expertise to handle cybersecurity. How can we be sure that our OT equipment is secure from cyber-attacks?"
- "I am the CFO at a 100-employee manufacturing operation looking at next year's budget with a priority in OT equipment expenditures which allow for higher production throughput. Cybersecurity sounds like an expensive and resource intensive initiative to undertake and I cannot afford a Cybersecurity consultant to come provide a custom solution. We are too small of a target for cyber-attacks so we can wait to prioritize a budget for cyber tools"
- "As a plant manager, I must prove that I have proper cybersecurity measures in place, or meet a specific industry standard, to be a supplier to multiple different customers. Otherwise, I risk losing their business on future contracts. How can I meet proper cybersecurity controls to ensure compliance and remain in their supply chain?"
- "As the owner of a small manufacturer, I just networked my machines as the first step towards reaping operational benefits from digital transformation on the shop floor. I know that my operations are not properly secure from Cyber-attacks. Without a cybersecurity engineer in-house and no budget for consulting support, I need to a user-friendly framework that my internal IT and operations resources can follow to secure my OT equipment."
- "As the IT director for a manufacturing plant, I purchased a new IoT for manufacturing solution and connected my shop floor with this new product. Our IT network infrastructure has proper cybersecurity, but this our first time bridging OT equipment with our IT networks. What data is being sent to my manufacturing equipment? Who has access to the data from my equipment? What tools can I use from IT cybersecurity in the OT environment?"
- "As an operations manager at a small manufacturer, I have been burned by expensive, long term custom cybersecurity implementations that constrained our options for what tools to implement. My internal personnel need user-friendly guides to lead them through the cybersecurity implementation process and give them lower-cost options. If we can gain more understanding internally, this will help us manage our own cybersecurity initiatives without costly options from a custom consulting solution."
- "I am an early adopter of digital manufacturing solutions and have a well networked shop floor, but the cybersecurity pieces we have in place are not comprehensive. There are a lack of regional manufacturing willing to share details about their cybersecurity program

to avoid oversharing of confidential information. Where can I get a detailed walkthrough and hands-on demonstration of a successful cybersecurity implementation?"

RFP Scope of Work

The above objectives must be completed within the following project constraints:
Period of Performance: 12 months
Anticipated MxD Funding: $500,000
Minimum Cost Share Contribution: $500,000

During the period of performance, the team should perform the initial market research as identified in the first objective to gain a deeper understanding of the problem space to de-risk their approach. The market research should not only take place at the beginning, but also revisited throughout the project performance. This will benefit the team by further refining the requirements for the deliverables and source additional existing research material that can be leveraged in the project.

MxD prefers a hybrid project management methodology which builds on traditional waterfall project planning and also employs agile methodology. This approach allows the project team to remain engaged with industry partners and/or consult with manufacturers throughout the period of performance to ensure the project work remains focused on value-add for the manufacturing sector, especially SMMs. Any opportunities to develop, validate, and refine project deliverables during the project will make for a more impactful project outcome.

Through an iterative development process, the proposal team will remain grounded in the real-world issues experienced in the manufacturing sector rather than determining an initial set of assumptions and carrying those through the entire project. Similarly, taking into account regular feedback from manufacturing companies will ensure that the project builds a business case and framework to prove the ROI which fits the needs of a manufacturing organization. MxD encourages close collaboration with an industry partner or multiple manufacturers to verify that the OT cybersecurity playbook will be successfully utilized by a manufacturing audience rather than an audience with cybersecurity expertise. It is a key requirement that the outcome of this project is geared to be user-friendly and easy to understand within the manufacturing community.

During the period of performance, the team will produce deployable deliverables that will be shared with the MxD membership in accordance with the Membership Agreement. The recommended deliverables are listed below in Table 1, but **the Proposal Team is encouraged to include additional deliverables or provide value-added changes to the recommended set of deliverables**.

IMPORTANT: If changes are made to the deliverables, the Proposal Team must provide the reasoning and detail any assumptions to provide context for the changes. Their proposed set of deliverables must align with MxD's focus on achieving deployable outcomes and enabling the transition of the research.

Table 1. *Technical Deliverables*

Deliverable	Description	Deliverable Due Date (Month #)

Documentation of SMM pain point discovery process	Document detailing approach for evaluating OT cybersecurity posture at manufacturing facility and criteria for prioritizing and identifying reasons for gaps in cyber security.	Month 1
Summary of top Cybersecurity hurdles	Report summarizing the findings of the discovery process. Technical report along with webinar content (i.e. slides and talking points).	Month 3
Documentation of ROI development process	Document detailing the manufacturing environment case study along with assumptions and constraints.	Month 3
ROI tool/framework	Framework for ROI calculations and/or software tool for custom ROI calculations.	Month 5
Validation of ROI tool/framework	Document detailing the ROI case study within a partner manufacturing organization	Month 5
Cybersecurity system architecture and framework	Technical report of the system infrastructure and integration framework. Including approach and diagrams.	Month 6
Developed playbook/framework	User-friendly version of a framework with clearly defined step-by-step guidance on how to develop a proper cybersecurity. Optional webinar content (i.e. slides and talking points).	Month 8
System architecture and implementation plans	Technical report of the system infrastructure and integration framework for the MxD implementation.	Month 9
Equipment identification and procurement plan	Detailed BOM (Bill of Material) that includes hardware and software specifications.	Month 9
System test and validation report	Validate proof of concept of system design and BOM by implementing and validating the system	Month
MxD implementation	Install and begin final preparation for demonstration at MxD factory floor.	Month 11
Implementation report	Technical report detailing implementation process. Story-telling based narrative presentation of this implementation process to demonstrate on the MxD Factory Floor	Month 12
Transition plan	Document detailing the hand-off to MxD Cyber team, MxD IT, and MxD engineering team. Include support details and ongoing costs such as licensing fees.	Month 12

The Proposal Team is expected to develop a transition plan, which is detailed in Table 2 in Section V. MxD is focused on supporting the transition of project outcomes to its membership in the form of pilot integrations on their factory floors, follow-on research projects or commercialized products available for use. Proposal Teams are expected to tailor their deliverables to their transition goals in order to provide outcomes that have continuing impact after the period of performance is complete. **Actionable transition plans are a priority for MxD to help maximize the benefits of funded research to the membership and ultimately, help increase the competitiveness of the US manufacturing base through new technological advancements. Thus, it is important that proposals emphasize not just technical merit but transition and deployment.**

mxdusa.org
@mxdinnovates
info@mxdusa.org

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

PROGRAM OVERVIEW

V. PROGRAM REQUIREMENTS

COLLABORATION

Participation in this program requires collaboration with a team of organizations with diverse capabilities. Competitive teams should optimally include representation from the manufacturing base, academia, solution/service providers and standards bodies. While it is not necessary for a proposing team to include all such organizations in their direct performers, MxD believes that involvement of diverse stakeholders increases the strength and applicability of project outcomes while reducing unforeseen risk.

Each Proposal Team must include participation by a manufacturer to drive use case and operational requirements. The manufacturer(s) are expected to define technical requirements, drive the business case for project outcomes. It is encouraged that the Tier 1 or Tier 2 Manufacturing Member provide the research testbed site but this is not required if an alternative location aligns better with the team's transition plan.

There is no requirement for a standards organization to be included on the Proposal Team but the Proposal Team is required to collaborate with industrial standards bodies to better inform their draft standards and help popularize their work to increase the potential for endorsement in the future.

The Proposal Preparation Information section outlines the opportunities that MxD provides to facilitate proposal team development:

- Teaming List: MxD will collect contact information from parties interested in teaming during the first weeks of the proposal period and will then disseminate the compiled list of contacts to the responders via email.
- Pitch Session: MxD will host a Pitch Session to provide organizations and/or teams the opportunity to share a snapshot of their solution approach and allow them to identify synergies with other interested parties.
- Participation in the Teaming List and Pitch Session is optional and NOT required in order to submit a proposal.

PROGRAM MANAGEMENT

MxD will be responsible for managing the project to ensure the team meets all the technical objectives and requirements proposed within the project's period of performance and budget. The MxD Project Manager will coordinate with Principal Investigators (PIs) of the Proposal Team to manage the program following MxD's project processes. The Director of Cybersecurity, in coordination with the assigned MxD Project Manager, will monitor technical performance and project costs of the associated Enterprise Award Agreement (EAA), the agreement that governs a project awarded by MxD to the Proposal Team Lead. Proposal Teams will submit the reports listed below in Table 2 to their identified Project Manager to fulfill their reporting requirements. These reports will be internally accessed by the MxD Director of Cybersecurity, the Government, the Project Manager and other authorized MxD staff members in the course of their official duties. Technology advancements will be summarized at least annually in order to support reporting to the Executive Committee, Technical Advisory Committee, MxD Members, and the Government, when applicable.

Table 2. Program Deliverables

Deliverable	Description
Project Immersion Workshop	Face to face meeting with manufacturer(s) including stakeholders from key business units to review project transition plan and define pilot requirements.
Transition Plan	Written plan for successful transition of project outcomes after period of performance including technology integration, educational distribution, and potential commercialization.
Monthly Technical and Financial Reports	Monthly report from the Project Team Lead including the financial and technical status of the project
Member Technical Reviews	Presentation encompassing all technical advancements made prior to key milestone and presented to the MxD Project Manager, members of the Technical Advisory Committee, and other interested MxD members.
Presentations at MxD	Presentation and demonstration of developed technology presented in person at MxD
Annual Patent Reports	Report of inventions and subcontracts
Intellectual Property Reports	Participants must promptly notify the MxD Project Manager apprised of Project IP created, filing status, claims against the Project IP, and BIP licensed to other Members.
Safety Accident/Incident Report	Participants must report any major accident/incident (including fire) resulting in any one or more of the following situations: one or more fatalities or one or more disabling injuries; damage of Government property exceeding $10,000; impact to Project planning or production schedules or degradation of the safety of equipment under contract. Such report will also identify potential hazards requiring corrective action.
Draft Final Technical Report	Draft report must include a comprehensive, cumulative, and substantive summary of all technical advancements and significant accomplishments achieved during the project.
Final Technical Report	See above
Project Team Lead Release	Release by Project Team Lead confirming scope of work to be complete
Property Report	List of all MxD funded equipment and planned disposition
Final Patent Report	Report of inventions and subcontracts

TRAVEL REQUIREMENTS

Proposals should include funding for up to four (4) trips per year for two (2) people for each member of the Proposal Team. These trips will be used for face-to-face meetings and presenting to the MxD membership. These trips may be for travel to MxD or to another location at the request of MxD (e.g., a conference, workshop, showcase, etc.). For estimation purposes, use Chicago, IL as the destination. Proposals may include additional funding for travel to the MxD Factory Floor for implementation and testing with proper justification.

PERIOD OF PERFORMANCE REQUIREMENTS

Proposed projects should be no more than twelve months in duration. Please note that projects are initiated once an EAA is signed, therefore, the project duration must include the subcontracting of all project participants between the Proposal Team Lead and each member of the Proposal Team.

Ownership of Deliverables and Intellectual Property

To accelerate digital adoption, cybersecurity, and workforce development across the U.S. manufacturing sector and to support the increased priority from our funding partners to transition project technology, MxD desires to own or co-own all the rights to intellectual property (IP) created during the project (Foreground IP or Project IP). It is the expectation that a member of the Proposal Team will co-own or will have a non-exclusive, non-transferable license to use the Foreground IP it creates. MxD will negotiate in good faith to achieve this result. MxD expects that the IP Management Plan (Attachment 1b) submitted with this proposal will reflect this position. MxD will have no rights to pre-existing intellectual property (Background IP) belonging to any member of the Proposal Team except as may be expressly agreed to in the Project documents. It is important to note that MxD will consider proposals that do not meet this request; proposals with IP Management Plans that reflect this will be favorably reviewed.

Funding Requirements

MxD anticipates awarding one project for no more than $500,000 of Federal Funding, not inclusive of required cost share, under the MxD-21-11 RFP. MxD reserves the right to fund all, some or none of the Technical Proposals received under issued RFPs. Final award amounts will be adjusted accordingly based on proposals received and subsequent evaluations.

This project requires a minimum 1-to-1 Cost Share in aggregate by the Proposal Team. For every dollar of Federal funding awarded, the Proposal Team must contribute at least a dollar of in-kind effort or cash. Thus, the Proposal Team in aggregate will need to provide at minimum 50% of the total project cost (inclusive of labor, equipment, materials, indirect, etc.) in cost share. This cost share can be in-kind or cash and can be distributed among the members of the Proposal Team however the team decides. Cost share must be accounted for in the cost proposal, as described in the Cost Development Guide found in the Proposal Preparation Kit.

Neither MxD nor the U.S. Government has any responsibility for costs associated with Technical Proposal or Cost Proposal development, submissions, or pre-award negotiations.

If down selected, the Proposal Team must submit substantiating documentation for all Proposal Team Member costs (including cost share) and MxD will complete a comprehensive cost analysis (including cost reasonableness and cost realism) prior to award. In addition, the Government Agreements office may conduct a cost analysis of all submitted cost proposals to approve the project. Approval of the Cost Proposal and Technical Proposal by the Government Agreements office and the DoD Program Manager is required for all MxD projects.

NOTE: Project award timelines are subject to approval of the project plan by the government and the allotment of funds from the government.

VI. ELIGIBILITY

MxD Membership

This RFP is open to the public; any organizations regardless of membership status may submit a Technical Proposal and Cost Proposal in response to this RFP. However, the MxD Membership Agreement must be fully executed with every Proposal Team member prior to project award. Any non-MxD members of the Proposal Team are encouraged to review the Membership Agreement prior to submission and to direct questions to MxD's Director of Business Development, Tony Papke (tony.papke@mxdusa.org). For more information on how to become 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 and cannot propose to RFPs in any capacity unless they address the following conditions:

- FFRDCs or Government entities may not exclusively team on any specific proposal team.
- FFRDCs must clearly 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, as well as, where relevant, contractual authority, establishing their ability to propose to solicitations utilizing government funding.

Government agencies interested in participating in MxD RFPs as part of Proposal Team should notify MxD in advance of Proposal submission. For RFPs utilizing Federal funding, special agreements and considerations may need to be implemented to enable participation.

Notification of Participation by Foreign Firms & Non-U.S. Citizens

Membership in MxD 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")).

Membership and project participation (or participation in projects without membership status) will be granted on a case-by-case basis at the sole discretion of the MxD Senior Leadership Team upon approval of the U.S. Government for any of the following:

- Any agency or instrumentality of a foreign government;
- Companies, firms, organizations, institutions, or other entities not organized or existing under the laws of the United States (as defined in Section 120.16 of the ITAR); and
- Non-U.S. Citizens.

In such event, all Members will be notified immediately of the foreign entity's role.

If a Member is a Corporation with subsidiaries or affiliates, its membership will include its wholly-owned and controlled and majority-owned and controlled U.S. subsidiaries and affiliates who qualify as a U.S. person under Section 120.15 of the ITAR.

It is a requirement that work related to the project must be completed in the U.S. by people legally authorized to work in the U.S. All proposed project participation by non-U.S. Citizens must be disclosed to MxD on Attachment 2c MxD Foreign Firms, Travel, & Non-U.S. Citizens at least 60 days prior to proposed participation. Written approval of foreign firms and/or non-U.S. Citizens must be received by the member of the Proposal Team from MxD prior to commencing work.

VII. TECHNICAL & COST PROPOSAL EVALUATION

EVALUATION PROCESS

An MxD Evaluation Board (EB) will review and evaluate each submitted Technical Proposal utilizing the evaluation criteria specified in the following section.

The EB may consist of recognized experts from industry and academia and key government stakeholder representatives (when appropriate). MxD representatives, such as the Director of Cybersecurity, and respective Project Managers, may participate in and lead EB meetings. All members of the EB will need to meet strict standards of personal and organizational conflict of interest. The evaluators may be supported by subject matter experts to review and comment upon the proposed work.

Through its deliberations, the EB will determine “selectability” of each submission. Selectability determination incorporates average EB score, judgement of market impact, and budget availability. The EB will identify a list of all proposed Technical Proposals that are “selectable for negotiation” leading to a subagreement award, along with their associated evaluation scores, to the Project Manager. The Director of Cybersecurity, with the consultation of other MxD representatives, will determine which subset of the proposed Technical Proposals deemed “selectable for negotiation” will be down selected for negotiations. This determination will take into account the EB’s recommendation, funding availability, alignment with MxD’s SIP as well as external stakeholder requirements (when applicable).

EVALUATION CRITERIA

MxD’s primary goal is to apply digital manufacturing technologies to solve business problems. To this end, successful proposers must demonstrate an understanding of both the business needs as well as the technology solutions. Proposals should provide a clear explanation of how the solutions address business problems and technical requirements outlined in the RFP, any assumptions, and considerations for deployment of developed solution through a pilot.

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

Proposal Evaluation Criteria	Order of Importance
Requirements Compliance • *Clearly articulates how the team will meet all the capabilities required by the RFP* • *Proposed solution clearly addresses problem statement and use cases identified in RFP* • *Clear identification of assumptions, risks, and mitigations; proposed deliverables align with requirements* • *Program management plan meets requirements in the RFP and is reasonable for the scope of work described in the technical proposal*	1
Methodology • *Clear and concise work effort scope targeted at problem statement* • *Proposed effort of direct relevance to RFP* • *Clear identification of barriers to implementation and explanation of how they will be overcome* • *Innovative methodology with high-potential for market impact* • *Significant and impactful use of external resources* • *Methodology demonstrates scientific and technical merit* • *SMART metrics and KPIs identified and described and demonstrate clear understanding of proposed work* • *Provides a maturity level assessment of both current and future state of technology with substantiation of assessed levels* • *Deliverables are fully described and identified*	2
Transition Plan • *Transition plan clearly articulates all project results and application into commercial and/or government products, systems and applications* • *Plan includes detailed descriptions of project results, risks/assumptions/mitigations, all required actions and timing, detailed funding and ROI strategy, key milestones, schedule and go/no-go decision points* • *Proposed team includes appropriate representation from researchers and industrial partners* • *Transition tasks and partners identified and thoroughly defined, both to MxD members and the broader industry* • *Solution and strategy to rapidly enable the adoption of the new technologies across the US manufacturing base is presented* • *Clearly defined IP ownership and innovative licensing strategies designed for rapid adoption of the new technologies* • *Discussion of future transition and/or commercialization demonstrates a clear understanding of the industry and possible markets for the technology* • *Benefits of project outcome are clearly defined and substantiated.*	3

Team Qualifications • *Members of proposed team are highly qualified to accomplish project tasks with clear delineation of roles and responsibilities* • *Solid evidence of commitment by team members, such as letters of commitment from their companies* • *Team members have unique capabilities that are directly associated with the target technology* • *Team includes a broad mix of capabilities and experiences to ensure success along with the commitment of top-tier facilities to accomplish all project tasks.*	4
Cost Factors • *Proposed cost estimates are reasonable and realistic for the proposed work effort* • *The minimum cost share proscribed in the RFP has been met or exceeded* • *Cost share is clearly defined and directly applicable to the performance and success of the project* • *Cost share value is readily discernable* • *Cost share from partners is documented with letters of commitment.*	5

VIII. PROJECT AWARDS

CONTRACT

MxD projects will be funded under the MxD Technology Investment Agreement (TIA), Contract Number W15QKN-19-3-0003 between MxD and the Government. All contractual negotiations related to RFPs will be executed by MxD. Funds will be distributed to the Proposal Team Lead selected through the evaluation/selection process utilizing an Enterprise Award Agreement (EAA). EAAs are usually Cost Reimbursement/Cost Share agreements; Milestone Payment/Cost Share based EAAs will be considered upon request.

MxD has provided an EAA template within the PPK for Proposal Teams to **review** prior to proposal submission. **The EAA should not be submitted with the proposal.** After receiving a notification of down selection, MxD will request the down selected Proposal Team to officially begin contract review and negotiations. MxD would prefer to execute an EAA only with the Proposal Team Lead. Once the EAA is executed, the Proposal Team can begin working on the project. When applicable, it is the sole responsibility of the Proposal Team Lead to issue contracts with applicable flow down clauses outlined in the EAA to any subcontractors, consultants, and any suppliers.

FINAL TECHNICAL PROPOSAL & COST PROPOSAL REVISIONS

MxD reserves the right to negotiate the cost and scope of the proposed work with the Proposal Team that has been down selected prior to award. MxD will facilitate the creation of a Statement of Work with the Proposal Team including technical scope modifications and program management aspects. All members of the down selected Proposal Team who intend to pursue selection are required to participate in the proposal revision process prior to award. For example, MxD may request that the organizations revise the technical scope to better align to RFP requirements.

mxdusa.org
@mxdinnovates
info@mxdusa.org

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

PROPOSAL PREPARATION INFORMATION

IX. PROPOSAL PREPARATION INFORMATION

This Proposal Preparation Information section offers detailed instructions on how to respond to this RFP; the Proposal Preparation Kit (PPK) includes the required proposal templates and reference documents on how to complete the templates. Together, the Proposal Preparation Information and PPK are intended to provide the basic information necessary for assembling complete proposals.

NOTE: MxD recommends Proposal Teams review the Request for Proposal Technical Summary & Program Overview prior to the PPK.

X. TEAMING OPPORTUNITIES

TEAMING LIST

To facilitate proposal teaming, MxD will collect contact information from parties interested in teaming during the first few weeks of the proposal period. MxD will then disseminate the compiled list of contacts to the responders via email and update on an ongoing basis as more contacts are added to the list. If you are interested in submitting your contact info to this distributed list, please email projects@mxdusa.org with the following information:

> ***"Subject: MxD-21-11 RFP Teaming***
>
> *[Organization Name]*
>
> *[Name of Contact]*
>
> *[Email address of contact]*
>
> *[1 sentence description of expected contributions to Proposal]*
>
> *I agree to have the information herein disseminated to other organizations that have indicated interest in teaming for MxD's RFP 21-11."*

PITCH SESSION

Additionally, MxD will host a **Pitch Session** on October 13, 2021 to provide organizations and/or teams the opportunity to share a snapshot of their solution and receive preliminary feedback from the MxD community. It will also serve as an excellent teaming opportunity for individuals and groups to identify synergies between their pitches. Pitch Session registration information will be posted at www.mxdusa.org/projects. Participation in the Pitch Session is not required to submit a Technical Proposal and Cost Proposal.

XI. SUBMISSION INSTRUCTIONS

SUBMISSION DETAILS

Each Proposal Team must submit their Technical Proposal and Cost Proposal no later than 5:00PM Central Time, November 18, 2021. All submissions must be made electronically to projects@mxdusa.org. Please include the RFP designation (e.g., "MxD-<XX>-<XX> – <RFP Title> - <Proposal Team> - <Proposal Title>") in the subject line of the email.

REQUIRED PROPOSAL DOCUMENTATION

The following section provides guidance on the necessary documentation, templates and submission formats required to submit a Technical Proposal and Cost Proposal in response to this RFP. Below are the documents (organized by PPK folder) that must be completed and submitted by the due date:

Required Proposal Documentation			
Title	**Document**	**Template**	**Submission Format**
Technical Proposal ONE PER PROPOSAL TEAM	Technical Proposal	Attachment 1a MxD Technical Proposal Template.docx	PDF
	Resume(s) of the Principal Investigator and Key Technical Personnel	N/A	PDF
	Letter(s) of Commitment	N/A	PDF
	Intellectual Property Management Plan (IPMP)	Attachment 1b MxD IP Management Plan.xlsx	XLS
Cost Proposal and Participant Certification ONE PER PROPOSAL TEAM	Cost Proposal	Attachment 2a Project Cost Proposal Template.xlsm	XLS
	Cost Narrative	Attachment 2b Cost Narrative Template.docx	PDF
	Certification of Foreign Firms, Travel and Non-U.S. Citizens	Attachment 2c Foreign Firms, Travel, & Non-U.S. Citizens.docx	PDF

- Each Proposal Team must submit **one Technical Proposal** (Attachment 1a). The instructions for completing the Technical Proposal are in the Technical Proposal template provided in the PPK folder. All questions are required, and attachments should be included.
- Each Proposal Team must submit **one completed IP Management Plan** (Attachment 1b) for the entire team with the Proposal. Instructions for completing the IPMP are provided in the template. The IPMP must contain Background Intellectual Property (BIP), Project (Foreground) IP, and assertions of limited rights to the Government.
- Each Proposal Team must submit **one Cost Proposal** (Attachment 2a) **including the Cost Narrative** (Attachment 2b) that is a summary or "roll-up" of all Proposal costs including cost share. Please reference the MxD Cost Proposal Development Guide for instructions on how to develop the Cost Proposal. An example Cost Proposal Excel Sheet and Cost Narrative are provided for reference. **Proposal Teams should be prepared to**

provide substantiating documentation for all Proposal Team Member costs within two weeks of down selection if the proposal is down selected. Additionally, if the proposal is down selected, the Proposal Team Lead must provide single audit results or other audited financials if Proposal Team Lead is not subject to single audit requirements.

- Each Proposal Team must submit **one Certification of Foreign Firms, Travel and Non-U.S. Citizens** (Attachment 2c) with information from every Proposal Team member. If there is personally identifiable information, separate certifications may be submitted
- The EAA is provided for review prior to submission. **The EAA should <u>not</u> be submitted with the proposal.**

Proposals that do not include the minimum requirements identified in the RFP will be deemed non-responsive and will not be evaluated.