The Digital Manufacturing Institute

MxD REQUEST FOR PROPOSAL

TECHNICAL SUMMARY, PROGRAM OVERVIEW and PROPOSAL PREPARATION INFORMATION

MxD-22-12:

Cybersecurity Standards & Guidelines for Protecting Operational Technology

Revision 1.0 Release Date: October 13, 2022

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	13 October, 2022	N/A	Original

II. PROJECT OVERVIEW

Project Type	TIA Enterprise Project
RFP Released	13 October, 2022
Team Formation List	Updated on Rolling Basis
Team Formation Opportunity (Optional)	8 November, 2022
Technical and Cost Proposal Due	12 January, 2023
Anticipated MxD Funding	$500,000
Minimum Cost Share Amount	$500,000 or requested funding amount, whichever is lower
Period of Performance	9 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.

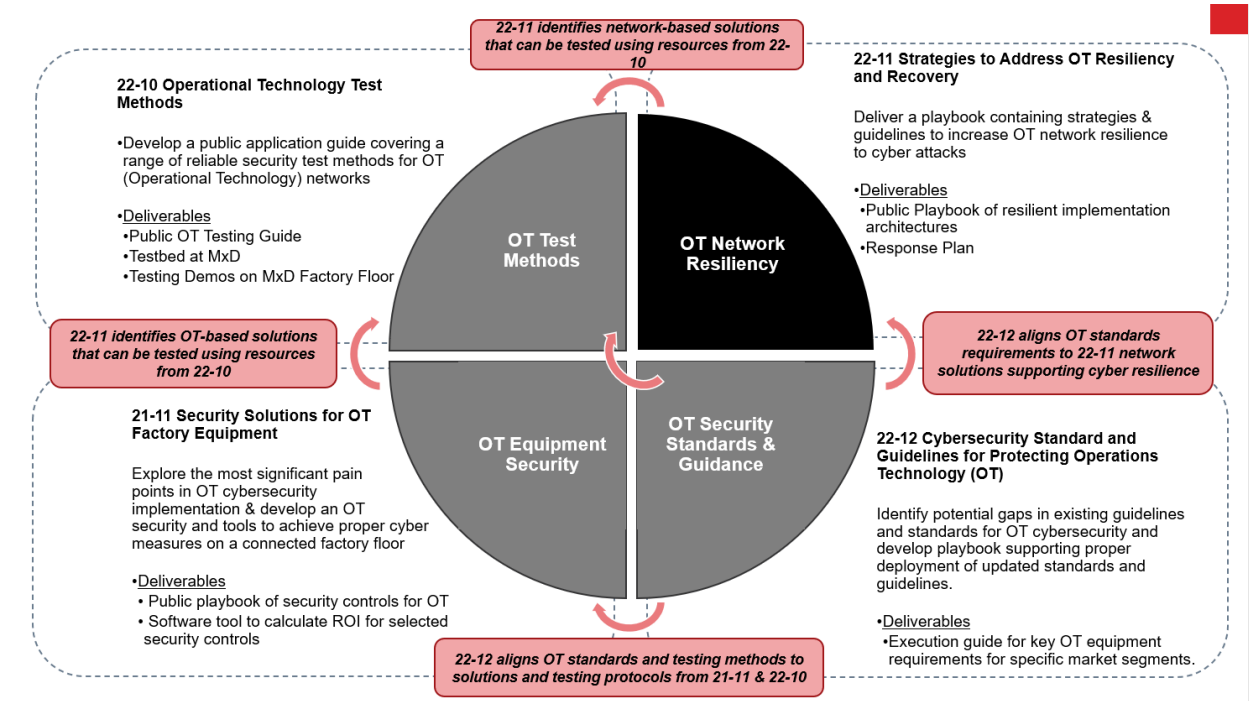
MxD has invested over $120 million in more than 85 applied research and development projects in areas including design, product development, systems engineering, future factories, agile and resilient supply chains, and cybersecurity.

MxD is also the DoD's National Center for Cybersecurity in Manufacturing. 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.

As a part of MxD's Strategic Investment Planning, MxD has launched several cybersecurity projects in 2022 that focus specifically on Operational Technology (OT) Security solutions and this is the latest in the series. These projects focus on four different aspects of securing OT, including Standards & Guidance for OT Security, OT Equipment Security, OT Network Resiliency, and Security Test Methods for OT. The following graphic describes the synergies of these projects and how the deliverables can be used in conjunction to identify, implement, and validate OT security solutions.



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

IV. TECHNICAL SUMMARY

PROBLEM STATEMENT

MxD was founded in 2014 with the mission to transform American manufacturing and accelerate the adoption of digital technologies throughout the manufacturing sector. Through this shift towards digital in this sector, there has been on emphasis on data connectivity across the entire enterprise to utilize operations data for improving operational efficiencies. The Operational Technology (OT) used in any manufacturing process can provide a rich stream of data from a connected factory floor. Along with the benefits that OT connectivity can provide an organization, there is also an expanded cyber threat surface and increased risk that a cyber event can occur. The benefits driven from data analytics has led many organizations to adopt digital solutions and take on increased cyber risk. Connected factory floors breakdown the traditional barriers that used to exist between the IT infrastructure and OT equipment. This convergence of IT and OT creates a new landscape of cyber risk management that most organizations are not familiar with in comparison to more traditional IT cybersecurity practices.

The traditional approach to cybersecurity on a manufacturing floor was air-gapping or keeping the manufacturing equipment disconnected from the IT infrastructure. IT systems are made up of devices that are frequently replaced or updated to address any cyber vulnerabilities with security patches. OT equipment such as PLCs, SCADA systems, and ICS devices have a much longer life span, and the process of security patching often requires a shutdown in production systems. To avoid interrupting operations, OT systems rarely receive necessary cybersecurity updates. Potential cyber threats extend from the IT systems into the OT environment when the two sides are connected in order to increase data visibility from the production operations. In addition to managing cyber risk within the IT infrastructure, these risks are now shared with the devices that make up the OT system.

Enterprise IT systems involve storage, recovery, manipulation, and transmission of data and cybersecurity is focused primarily on the confidentiality of this data along with availability. Cybersecurity practices for IT systems are more well developed with various standards and compliance frameworks in place. These standards include NIST 800-171 and CMMC to protect data in the manufacturing sector, PCI DSS to protect payment information, and HIPAA protecting personal health information. These standards have been broadly adopted across various industry sectors and deployed to support data confidentiality per compliance requirements. An OT network is made up of production equipment that drives operations, therefore the focus of cybersecurity in a manufacturing environment is on equipment availability and safety to prevent any cyber events from interrupting operations or damaging the physical equipment. There are some guidelines and standards developed to address OT infrastructure cybersecurity, including ISA/IEC 62443, NIST CSF, and NIST 800-53. With a lack of compliance requirements for cybersecurity in OT systems, these standards lack widespread adoption within the manufacturing sector.

Despite a growing awareness of cyber vulnerabilities within OT systems and recent headlines highlighting the impact that a cyber threat can cause an organization, many manufacturing organizations have not implemented proper OT cybersecurity measures. Specifically, within the small-to-medium manufacturing (SMM) community, the resources are not available to dedicate time or personnel to navigate the standards landscape and find proper guidance for their internal

OT cybersecurity implementations. While some manufacturers are more advanced in their cybersecurity practices in their operations environment, it is critical that all sizes of manufacturing organizations have the tools to adopt proper cybersecurity measures. This will build a more robust supply chain within the DIB and broader manufacturing community with fewer risks to supply chain disruptions due to cyber vulnerabilities and threats. MxD has identified an opportunity to help accelerate the adoption of cybersecurity practices through simplifying the existing standards and guidelines in the OT landscape.

MxD is funding a project to explore the current landscape of OT cybersecurity compliance standards and industry guidelines, identify best practices from these to summarize and simplify this information for the SMM audience, and demonstrate these practices in a playbook. To drive specific value in this effort, MxD would like to narrow the scope of this effort down to the cybersecurity of physical equipment on the manufacturing floor rather than accounting for cybersecurity across an entire enterprise. In reference to the Purdue Model, the area of focus should be level three down to level zero to include ICS and SCADA systems, PLCs and RTUs, and process sensors and actuators. The body of knowledge in OT cybersecurity is very extensive and hard to digest without a clear starting point. MxD is looking to leverage this existing knowledge to provide simplified guidance to the manufacturing community without re-inventing the wheel or developing cybersecurity standards.

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. Mapping the current state of the art in OT cybersecurity standards and frameworks at the lower levels of the Purdue Model, focusing on levels zero through three. The project should explore the landscape of guidance currently being followed by various players in the manufacturing space, from OEM machine tool builders to system integrators and end users of OT equipment at manufacturing organizations.

   The requirements for this objective are as follows:

   - Explore the industrial standards and frameworks which are being utilized for OT devices within the manufacturing sector. Summarize the scope of these standards.

- Document how the existing standards apply across different manufacturing verticals and compare how adoption of these frameworks varies across different verticals.
- Determine if there are OT cybersecurity standards from other industries outside of manufacturing which may be applicable within the manufacturing sector.
- Investigate decision factors that manufacturing organizations take into account for selecting a framework for their internal OT cybersecurity (i.e., compliance requirement or level of effort to implement).
- Summarize this discovery phase effort in a report detailing the current state of OT cybersecurity in the manufacturing industry.
- The findings of this initial investigation should continually be revisited throughout project performance to ensure that further objectives accurately reflect the real-world situation manufacturers face.

2. Derive common cybersecurity best practices playbook for OT hardware from existing standards and frameworks. Building on the outcome of the first objective, the project should identify commonalities across the requirements of existing standards and guidance to summarize these into a playbook or framework for OT equipment cybersecurity best practices. If applicable, additional guidance and best practices can be developed beyond existing standards or frameworks to help address any gaps and move the industry forward.

   The requirements for this objective are as follows:

   - Develop a crosswalk of standards to illustrate where the overlap is. This crosswalk should include a high-level summary version for non-technical audiences along with a more detailed report on this crosswalk.
   - Document the broadly applicable cybersecurity practices that can be utilized in an OT environment regardless of manufacturing vertical.
   - Define the industry specific practices that certain manufacturing sectors or verticals should consider apart from the broadly applicable practices.
   - Map all best practices and guidance to the existing frameworks and compliance standards discovered in the first objective.
   - Should not be solution specific but take into consideration the categories of cyber solutions that can be utilized to support the best practices.
   - Consider the feasibility of deploying each of the best practices when faced with the real-world hurdles of the manufacturing sector and specifically the challenges of SMMs adopting cybersecurity practices.
   - OT equipment cybersecurity best practices framework should cater to an SMM audience and provide practical guidance while stripping away the compliance standards technical language.

3. Demonstrate the proper application of OT equipment cybersecurity best practices. With a complete understanding of the existing OT cybersecurity governance space and additional guidance developed, the project should demonstrate these outcomes for the manufacturing sector. This could take the form of a pilot deployment of the project findings

or furthering objective two and developing an execution guide for key manufacturing market segments.

The requirements for this objective are as follows:

- Develop a framework for how the playbook will be utilized for a pilot implementation of the best practices.
- Determine how the theoretical best practices work within the real-world complications of a manufacturing operations environment.
- Report on the challenges experienced, decision factors, and lessons learned through the implementation process.
- Document the assumptions of this implementation and consider how the approach would have to be customized for implementation across different manufacturing verticals.
- Prepare a case study to capture the exercise of implementing new cyber practices, lessons learned in the process, and report on project KPIs.

Through these objectives, the project principally seeks to address the following use cases:

- "As the owner of a small manufacturing organization, we have invested in cybersecurity measures within our IT infrastructure to prepared for cyber threats but have newly connected our OT equipment to the enterprise network for data visibility. What guidance is there for cybersecurity in manufacturing OT systems?"
- "As an IT manager at a defense industrial base supplier, we are starting our cybersecurity implementation to reach CMMC compliance for data confidentiality per contractual requirements. How do the cybersecurity controls put into place for CMMC compliance help to protect my production equipment from a cyber threat interrupting operations?"
- "As a systems integrator in the manufacturing sector, what cybersecurity practices should I deploy within a manufacturing client facility to ensure equipment safety and availability in the absence of cybersecurity compliance requirements for their OT infrastructure?"
- "As an operations manager at a small machine shop, we want to utilize digital technologies for increasing production efficiencies. Before I network my OT equipment to support my digital manufacturing transition, what guidance can I follow to ensure my OT network is built with cybersecurity best practices in place?"
- "As an OT device manufacturer and supplier looking for a competitive advantage in the market, can I build in any cybersecurity measures that will support proper cyber practices according to various frameworks and standards being utilized within the manufacturing sector?"

RFP Scope of Work

The above objectives must be completed within the following project constraints:
Period of Performance: 9 months
Anticipated MxD Funding: $500,000
Minimum Cost Share Contribution: $500,000

During the period of performance, the team should perform the initial industry research as identified in the first objective to gain a deeper understanding of the problem space to de-risk their

approach. The industry 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 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 organizations will ensure that the project builds a playbook and set of guidance which fits the needs of the manufacturing community. MxD encourages close collaboration with an industry partner or multiple manufacturers to verify that the project outcome 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 Proposal 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 #)
Current landscape of OT cybersecurity standards and guidelines	Technical report documenting the cybersecurity compliance standards and frameworks being utilized within the manufacturing sector. Summarize these standards and how they are utilized within OT systems.	3
OT cybersecurity standards and guidelines crosswalk	Document the areas of overlap and unique aspects of the standards and frameworks of manufacturing OT cybersecurity. Should be developed for a non-technical audience.	4
Common best practices from existing guidance	Technical report on mapping and documenting best practices for OT	5

	cybersecurity to the different industry standards.	
Playbook	Training material describing how to implement cyber measure best practices catering to the SMM community.	6
Framework for deployment	Documenting a plan for how the playbook will be used in practice and steps for deployment in a pilot factory.	6
Lessons learned in deployment in factory floor	Report on the challenges experienced, decision factors, and lessons learned when implementing cybersecurity practices per playbook guidance.	9
Transition Plan	Documentation of how this project outcome will be transitioned to the broader manufacturing community. Can include training videos, education materials, webinars, etc.	9

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. **Pilot deployments and 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 include representation from the manufacturing base, academia, solution/service providers and standards bodies.

Each Proposal Team should 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 and serve as a pilot manufacturer for test and validation of the solution. 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:

- Team Formation List: MxD will collect contact information from parties interested in forming a team during the first month of the proposal period and will then disseminate the compiled list of contacts to the responders via email.
- Team Formation Opportunity: MxD will host a Team Formation Opportunity 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 Team Formation List and Team Formation Opportunity 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 Senior Director of MxD's Project Management Office (PMO), 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 Senior Director of MxD's PMO, 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 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 pilot site for implementation and testing with proper justification.

Period of Performance Requirements

Proposed projects should be no more than nine 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-22-12 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 within 30 days of notification of project down select; acknowledgement of this is required in the Technical Proposal submission. Additionally, any organizations which are already members of MxD must ensure they are a member in good standing within 30 days of notification of project down select.

Any non-MxD members are strongly encouraged to conduct a legal pre-review of the Membership Agreement prior to submission as this is a common source of delay during negotiations with proposal teams that have been chosen during down selection. Please 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. If any member of the proposal team is not either a U.S. citizen or a lawful permanent U.S. resident (green card holder), please reach out to MxD at projects@mxdusa.org before submitting a proposal. 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 Senior Director PMO, 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 Senior Director, PMO, 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 supply chain, 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 technology 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. **The EAA must be fully agreed with the proposal team lead within 60 days of down selection notification;** acknowledgment of this is required in the Technical Proposal submission. 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. TEAM FORMATION OPPORTUNITIES

TEAM FORMATION LIST

To facilitate proposal team formation, MxD will collect contact information from parties interested in forming teams during the first month of the proposal period. MxD will then disseminate the compiled list of contacts to the responders via email. If you are interested in submitting your contact info to this distributed list, please email projects@mxdusa.org with the following information:

> ***"Subject: MxD-22-12 RFP Team Formation***
>
> *[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 forming a team for MxD's RFP 22-12."*

TEAM FORMATION OPPORTUNITY

Additionally, MxD will host a **Team Formation Opportunity** on November 8, 2022 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 opportunity for individuals and groups to identify synergies between their pitches. Team Formation Opportunity registration information will be posted at www.mxdusa.org/projects. Participation in the Team Formation Opportunity 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, January 12, 2023. All proposals must be submitted via the MxD website. The SUBMIT button can be found on each RFP webpage at www.mxdusa.org/projects. By clicking the SUBMIT button, applicants will be directed to the official Submission Form.

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.