The Digital Manufacturing Institute

MxD REQUEST FOR PROPOSAL

TECHNICAL SUMMARY & PROGRAM OVERVIEW

MxD-19-12:
Cybersecurity Tools Pilot Program

Revision 1.0 Release Date: November 12, 2019

Contact: Akin Akinbosoye
Director, Cybersecurity
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	01 November 2019	N/A	Original
2.0	29th January, 2020	Eligibility Contact	Language regarding the requirement of work being completed inside the U.S. added to the RFP Updated contact: Akin Akinbosoye

II. PROJECT OVERVIEW

Deadline for Submitting Interest in Teaming	5 PM CST, 05 December 2019
Proposals Due	5 PM CST, 12 February 2020
Anticipated MxD Funding	$200,000
Period of Performance	9 months

III. INTRODUCTION

MxD: The Digital Manufacturing Institute (formerly the Digital Manufacturing and Design Innovation Institute – DMDII) 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. As a result, our nearly 300 members increase their productivity and win more business.

MxD has invested approximately $90 million in more than 60 applied research and development projects in areas including design; product development; systems engineering; future factories; agile, resilient supply chains; and cybersecurity.

MxD operates from a nearly 100,000-square-foot innovation center near downtown Chicago. Its 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 Request for Proposals (RFP) are issued to address research and development needs in digital design and manufacturing technology that are aligned with the technical objectives of MxD and directly support the Institute's vision of developing digital manufacturing systems that make every part better than the last.

This RFP contains the following elements:

1. Request for Proposal Technical Summary & Program Overview: a description of a specific technology objective and technical and program requirements

2. Proposal Preparation Kit (PPK referenced as the Kit): includes a PPK overview document and attached proposal templates and references. The PPK Overview provides background and guidance for the preparation of required forms and instructions needed to submit to a MxD Request for Proposal. The PPK Overview offers detailed instructions on how to respond to this RFP and provides attachments with the required proposal templates. It is intended to provide the basic information necessary for assembling complete and compliant proposals and to help explain those areas that usually generate the most questions from Offerors.

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

The RFP is available on the MxD website at http://mxdusa.org. Notices announcing MxD competitions and due dates will also be posted on the MxD website. Amendments to a MxD RFP may be used to extend due dates, clarify procedural requirements or modify technical requirements. An updated RFP may be issued, and the previous RFP will be rescinded. Offerors should carefully monitor the MxD website subsequent to 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 Offeror 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.

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.

IV. PURPOSE

MxD will periodically solicit proposals for applied research and technology development to meet the goals outlined in its Strategic Investment Plan (SIP) or complementary goals specified by key external stakeholders that align with MxD's core mission. The process by which this achieved is through an RFP.

An 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. The purpose of an RFP is to solicit proposals for projects in technology areas that are of interest to MxD membership and external stakeholders such as the U.S.

Government. MxD will initiate and coordinate development of the RFP topics by engaging Technology Advisory Committee (TAC) members, MxD's Agile Tech Team, Department of Defense (DOD) affiliates, and other relevant stakeholders. Once the RFP topics are developed and approved the MxD RFP will be posted to the MxD website and represents the official notification to Offerors of a request to submit the required documents.

mxdusa.org
@mxdinnovates

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

REQUEST FOR PROPOSAL
TECHNICAL SUMMARY

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

V. TECHNICAL SUMMARY

PROBLEM STATEMENT

Digital transformation of manufacturing processes leaves it vulnerable to cyber-attack. There is a lack of tools and expertise needed to identify and mitigate these risks, especially for SMMs in the supply chain. With the lack of expertise, tools for the security of manufacturing assets and the continuing digitization and connectedness of manufacturing equipment, manufacturers require a new paradigm. One that includes the capability to identify vulnerabilities in information and operations technologies that enable manufacturing operations; This problem is amplified in small and medium manufacturers that make up 98% of the American manufacturing supply chain. Many small and medium-sized manufacturers are unaware of federal requirements and may lack the financial and technical capabilities required to manage cybersecurity.

Moreover, traditional vulnerability assessment tools have targeted the discovery, validation, and testing of vulnerabilities in information technology systems. Digital manufacturing has continued to increase the use of technologies including connected systems in traditional manufacturing equipment. Increased connectivity and data-driven/aided manufacturing brings risks that were primarily associated with information technology to the operations technology space. Solutions to be tested therefore must have capabilities that allow for testing of operations technology and information technology (OT/IT) components of manufacturing entities.

To address challenges with ease of deployment and use, and cost-effective solutions for small and medium manufacturers in the supply chain, MxD is releasing a Request for Proposal for the benchmarking and evaluation of user-friendly (consumer-grade), intuitive and effective cloud-based tool and/or toolset for cataloguing, assessing vulnerabilities and automated penetration testing of IT/OT assets for small and medium-sized manufacturers in the supply chain. These objectives are consistent with the requirements in the NIST Cybersecurity Framework (Version 1.1) for the identification and protection of assets (OT/IT assets). Where protection measures are informed by the risks associated with the information and data about each of the assets or classes of assets in the operating environment.

Furthermore, the RFP seeks to benchmark existing solution(s) based on a set of criteria that have been defined and others that may be added by each of the evaluation teams. Expected output may include gaps in capabilities and/or opportunities for enhancements to existing tools to better meet the needs of the users in the supply chain. Modifications or changes to solutions included in this benchmark are not in scope for this RFP.

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

OBJECTIVES AND TECHNICAL REQUIREMENTS

Findings from this project will inform decisions regarding adoption, augmenting/enhancing, and/or integrating capabilities within a tool or collection of tools; the project's objective is to evaluate Penetration and Vulnerability assessments tools with a focus on total cost of ownership; ease of deployment and use; effectiveness; and efficiency.

The above objectives must be completed within the following project constraints:
Period of Performance: 9 Months
Anticipated MxD Funding: $200,000

The team will provide anonymized/de-identified results of vulnerability assessment and automated penetration tests from a minimum of 5 manufacturer (for diversity of participants, the team is strongly encouraged to include as many small and medium-sized manufacturers as possible – no more than 10 manufacturers) with 500 or fewer employees generated by the tools that are included in this pilot with the goal of evaluation on established criteria in Table 1.

Each team is required to perform the following task to achieve the objectives within the scope of work:

Development or Identification of Cybersecurity Profile for Manufacturers: Develop or leverage existing literature for self-assessment profiles that helps manufacturers understand their current cybersecurity readiness/status and their unique needs relating to cybersecurity toolsets.

i. The self-assessment should be able to be completed by an IT professional with assistance from manufacturing, ops, etc.
ii. The manufacturing profile should take no longer than 4 hours to complete.
iii. The profile should consider the number of employees, device types, and other factors each team deems necessary.

Define/document criteria for benchmarking of existing Cybersecurity solutions: Create a set of criteria that is vital to an effective SMM cyber solution and benchmark tools that meet the proposed minimum technical requirements (see section on minimum technical requirements for applicable descriptions). This benchmarking framework should also act as a standalone tool so SMMs can utilize to do their own benchmarking after the project. It is anticipated that initial solution could be in a spreadsheet with potential for porting for web-deployment for easier/broader accessibility by members.

Report(s) on performance of benchmarked tool(s)based on established criteria: Conduct a pilot implementation and test of the top cybersecurity tools for vulnerability management and non-intrusive penetration testing from the benchmark assessment that matches the SMM's cyber profile. The pilot implementation will be analyzed to validate the effectiveness of the benchmarking, identify solution gaps, and provide

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

guidance for implementation that will help inform tool(s) selection and usage by SMMs in the supply chain.

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 2, but the 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 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.

Through these objectives, the project seeks to address the following use cases and others that participants find relevant to the operations of the manufacturers in the supply chain:

1. As the person responsible for implementing our cybersecurity program at a small manufacturer, I want a resource that will not only tell me I have a problem but also point me in the right direction for how to address the issue so I can be confident that the risk has been reduced.

2. As the person responsible for implementing our cybersecurity program at a small manufacturer, I want easy-to-use tools that can be easily understood without taking too much time away from my day job.

3. As the supply chain manager at a large manufacturer, I want to be confident that my suppliers are improving their cybersecurity practices to reduce cybersecurity risks across my supply chain(s).

Minimum Technical Requirements:
Proposals should meet the following minimum technical requirements:

Asset Discovery and Inventory
Inventory/catalogue Client Technology (IT/OT) assets and resources (e.g., applications, database, endpoint devices, network appliances, OT equipment/appliances, and servers), as required for assessment/testing scope determination.

Network Vulnerability Assessment/Test
Assess current network security measures to identify any vulnerability that exists in the Client's network infrastructure. Conduct external and/or internal scans/tests to identify any security vulnerability that exists in the Client's assets and resources.

Application Vulnerability Assessment/Test
Conduct web application security assessment and wireless security assessment.

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

Automated Report Creation
Create an automated report of security findings with assessed criticality ratings and recommendations for remediation.

Table 1. Evaluation Criteria/Key Performance Indicators

Key Performance Indicators	Description
Total cost of ownership	Relatively low acquisition cost and ongoing maintenance and support costs to operators.
Ease of deployment	Relative ease of deployment (cloud-based) of the assessment tool(s) for users with minimal technical expertise.
Ease of use	Measured by usability of tool(s) for small to medium-sized manufacturers with limited resources and expertise.
Effectiveness of the tools	Measured in terms of accuracy in identifying vulnerabilities with a low rate of false positives, and risk ranking of findings for prioritization of remediation efforts.
Intuitiveness/Efficiency	Recommendations for remediation of vulnerabilities must be in simple, easy to follow steps for implementation.
Non-Intrusiveness of Solution(s)	Solutions will be evaluated based on minimal to no impact on regular operations from use in the manufacturing plant.
Provider viability Assessment	Solution provider(s) for selected tools should be assessed for sustainability of business model and practices

Table 2. Recommended Deliverables

Deliverable	Description
Manufacturer Profile	Documented profiles for the manufacturers included in the pilot to help manufacturers with assessment of adoption decisions.
Defined/documented criteria for Benchmarking of Existing Cybersecurity Solutions	Documented set of criteria that is vital to an effective SMM cyber solution and benchmark tools on the listed functional/technical evaluation factors.
List of tools considered for evaluation	A list of candidate tools considered for inclusion in the evaluation for the established criteria
Criteria for selection of evaluated tool(s)	Criteria used for the determination of the tool(s) selected for use in the evaluation exercise.

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

Report(s) on performance of benchmarked tool(s) based on established criteria	Report from pilot implementation detailing analysis to validate the effectiveness of the benchmarking, identify solution gaps, and provide guidance for implementation that will help maximize ROI for SMMs.
De-Identified/Anonymized Results of vulnerability assessment and penetration test(s)	Summary of anonymized (de-identified) results from instances of vulnerability assessment exercises.
Prioritized recommendations	Report with prioritized recommendations for the remediation of identified vulnerabilities.
Evaluation Scorecard	Results from the team's evaluation of tool(s) based on established criteria.
Due Diligence Report	A report of due diligence performed to assess the longer-term viability of vendor(s) for selected tools (financial standing, business model and roadmap for enhancements and updates are critical considerations).
Installation and configuration guide	Guide providing user instructions for installation and configuration of the system.
Software guide	Guide providing user instructions for software use.
User guide	Guide providing user instructions for calibration and operation of the system.
User training and DEMO (online webinars, training)	Instruction material, coaching, and feedback to prepare those who deliver training, including full-time trainers, and managers, either in a classroom (physical or virtual) or on-the-job setting.

The team is expected to develop a transition plan, which is detailed in Table 3 in Section VI. 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. 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

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

PROGRAM OVERVIEW

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

VI. 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, solution/service providers, academia and manufacturers (of varying sizes).

Use cases provided in the objectives and scope section are not exhaustive, the offeror team(s) is encouraged to provide complementary use case(s) within the scope established in the scope and objectives section for demonstration or provide requirements for an additional deliverable that shows how this project offers tangible value to the SMM community. Each team must include participation from small or medium manufacturer. The expectation is that teams will obtain input/feedback on the tools and evaluation process from a minimum of 5 small and medium-sized manufacturers (with 500 or fewer employees).

Solution Providers may be enlisted to help advise, assist with implementation and evaluation of existing cybersecurity solutions to identify how these solutions meet or fall short of meeting the needs of SMMs by embracing consumer (user) experience paradigms, tailoring solutions that are effective and efficient for vulnerability assessment and penetration testing in OT/IT environments, and incorporating key learnings from this cybersecurity pilot program.

Participation by MxD's tier I and II members are encouraged to assist with the recruitment of SMMs in their supply chains for adequate diversification of use cases and broaden participation across differing organization sizes. Teams are also encouraged to have appropriate representation from academia. The role of the Academia will be to assist with the structure and content of the white paper(s) and other technical reports to be produced; and identify additional research opportunities.

Offeror teams are encouraged to actively seek opportunities for leveraging existing standards from NIST and other relevant standards bodies. There is no requirement for a standards organization to be included on the offeror team, but the offeror team may collaborate with standards bodies to better inform future and/or updates to standards and help popularize their work to increase the potential for adoption across industry.

PROGRAM MANAGEMENT

MxD will be responsible for managing the project to ensure their team will meet all the technical objectives and requirements proposed within the project's period of performance and budget. The MxD Project Engineer will coordinate with Principal Investigators (PIs) of every participant to manage the program following MxD's project processes. The Director of Cybersecurity, in coordination with each project's MxD Project Manager, will monitor technical and cost performance of the associated

Enterprise Award Agreement. Project teams will submit the reports listed below to their identified Project Engineer 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.

Deliverable	Description
Project Immersion Workshop	Face to face meeting with solution provider 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 each Project Participant 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 Engineer, 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 Engineer 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

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

Travel Requirements

Proposals should include funding for two trips for 2 people 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 manufacturer sites for implementation, testing, profile development and other required activities 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 Enterprise Award Agreement is signed, therefore, the project duration must include the subcontracting of all project participants between the Lead Organization and the Project Participants. For this project MxD will enter into an Enterprise Award Agreement with each Project Participant individually such that no Project Participant will be a contracting Lead Organization.

Funding Requirements

MxD anticipates awarding one project for $200,000, not inclusive of expected cost share, under the MxD-19-12 RFP. 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 each Offeror team.

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

VI. ELIGIBILITY

MxD Membership

All organizations selected to participate on projects must be MxD Members, in accordance with the MxD Membership Agreement, prior to project award. This RFP is open to the public; any organizations regardless of membership status may submit a Technical Proposal and Cost Proposal in response to an RFP. MxD, in its sole discretion, may make the Membership Agreement effective upon project selection and require payment of the membership dues. The Membership Agreement must be fully executed with every participant within 30 days of project selection. Any non-members Offerors are encouraged to review the Membership Agreement prior to submission and to direct questions to the MxD 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 project 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 an Offeror team should notify MxD in advance of Proposal submission. For RFPs utilizing Government funding, special agreements and considerations may need to be implemented to enable participation.

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

As required by the Technology Investment Agreement, 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”)). All proposed project participation by Non-U.S. Citizens must be disclosed to MxD at least 60 days prior to proposed participation for approval.

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

Membership & project participation (or participation in projects without membership status) will be granted to 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 on a case-by-case basis at the sole discretion of the Executive Committee upon approval of the U.S. Government. In such event, all Members will be notified immediately of the foreign entity's role.It is a requirement that work related to the project must be completed insdie the U.S.

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.

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. Cost Proposals will not be provided to the Evaluation Board for the purposes of evaluation. Cost Proposals will be utilized by MxD and the Government during the cost analysis and project approval process.

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 Manager, 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 sub agreement 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 SIP as well as external stakeholder requirements (when applicable). MxD reserves the right to fund all, some or none of the Technical Proposals received under issued RFPs.

If down selected, 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 Cost Proposals. Approval of the Cost Proposal and Technical Proposal by

the Government Agreements office and the DoD Program Manager is required for all MxD projects.

Cost share is required for all MxD projects that are executed through the MxD. Cost sharing or matching relates to the portion of project or program costs supported by the Offeror and not by MxD.

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.

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

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

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 Tech Investment Agreement 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 those offerors selected through the evaluation/selection process utilizing Enterprise Award Agreements (EAAs). EAAs are Cost Reimbursement/Cost Share agreements.

MxD has provided an EAA template within the PPK for Offerors 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 all down selected project

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

participants to officially begin contract review and negotiations. MxD will execute EAAs with every Offeror organization individually (i.e. MxD will function as the Project Prime/Lead) and all EAAs will share the same Statement of Work and Intellectual Property Management Plan. Once the EAA is executed the project team can begin working on the project. When applicable, it is the sole responsibility of Offeror organizations to issue sub-awards to any subcontractors and to ensure team members are abiding by the terms and conditions within the EAA.

Final Technical Proposal & Cost Proposal Revisions

MxD reserves the right to negotiate the cost and scope of the proposed work with the project participants that have been down selected prior to award. MxD will facilitate the creation of a Statement of Work with all participants including technical scope modifications and program management aspects. All down selected organizations 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. Neither MxD nor the U.S. Government has any responsibility for costs associated with pre-award negotiations.