



The Digital Manufacturing Institute

MxD

REQUEST FOR INFORMATION

Supply Chain Illumination for a Resilient Industrial Base

Revision 1.0 – August 18, 2026

Program Contact: Scott Kruse
scott.kruse@mxdusa.org

MxD
1415 North Cherry Ave
Chicago, IL 60642

TABLE OF CONTENTS

Record of Change.....	3
Key Dates	3
Introduction	3
RFI Subject	3
Purpose	3
Policy Context.....	4
Background and Problem Statement.....	4
Working Definition & Scope.....	5
Capability Areas of Interest	5
Respondent Profile	5
Information Requested.....	6
Questions for Respondents.....	6
Response Format and Limits	8
Submission Instructions	8
Disclaimers	8

RECORD OF CHANGE

Revision	Date	Sections	Description
1.0	August 18, 2026	N/A	Original

KEY DATES

RFI Released	August 18, 2026
Deadline for submissions to be received	September 4, 2026 8 PM CT

INTRODUCTION

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

MxD has invested over \$400 million in more than 200 applied research and development projects in areas including design, product development, systems engineering, factory modernization, agile and resilient supply chains, workforce training, and cybersecurity.

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

This RFI is publicly available on the MxD website at <https://www.mxdusa.org/solicitation-opportunities/>. This public posting represents the official notification of a request to submit the required documents. Amendments to an MxD RFI may be used to extend due dates, clarify procedural requirements, or modify technical requirements. If an updated RFI is issued, the previous RFI will be rescinded. Those interested in responding to this RFI should carefully monitor the MxD website after an original posting, up to the time of the submission due 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 Respondents to monitor the MxD RFI updates and ensure that their submission meets all information requirements.

Any questions regarding this RFI must be provided to scott.kruse@mxdusa.org

RFI SUBJECT

This RFI seeks information on existing, emerging, and transferable approaches to attaining actionable visibility across multi-tier supply chains. The primary lens is the defense and aerospace industrial base, and MxD also welcomes relevant practices and lessons from other critical manufacturing sectors.

PURPOSE

MxD is seeking input to identify practical pathways for improving multi-tier supply chain visibility across the defense and aerospace industrial base and adjacent manufacturing sectors. The goal is to connect demonstrated capabilities, implementation experience, and emerging approaches with actionable needs across the MxD ecosystem.

Responses that will help MxD:

- Identify approaches that organizations can implement today and capability gaps requiring further development.
- Define priority use cases and the technical, operational, and governance conditions needed for successful implementation.
- Identify potential pilot or demonstration concepts that could validate value, feasibility, scalability, and supplier participation.
- Inform practical guidance, collaborative initiatives, applied research and development, partner programming, or recommendations for industry and government stakeholders.
- Surface opportunities for manufacturers, suppliers, solution providers, and other ecosystem partners to contribute to future MxD-led activities.

Through this RFI, respondents have an opportunity to shape how MxD prioritizes and pursues practical supply chain visibility efforts. This RFI does not commit MxD to a specific project, acquisition, technology approach, funding opportunity, or follow-on solicitation.

POLICY CONTEXT

On July 20, 2026, Executive Order 14415, [Securing America's Defense Supply Chains and Ensuring Domestic Acquisition of Critical Materials](#), established a policy of securing defense supply chains against physical, cyber, and economic subversion. Among other actions, the order directs development of policy and implementation guidance for mapping and illuminating critical supply chains across contractor tiers, from raw materials to end-use products.

The order contemplates complete indentured bills of materials; proactive vetting of suppliers for financial, foreign ownership/control/influence, and manufacturing and supply risks; timely mitigation and corrective-action processes; and analysis of vulnerabilities, bottlenecks, and single points of failure. It also directs that implementation account for the ability of small businesses, non-traditional defense companies, and new entrants to comply without undue burden.

Please note, this RFI is not an interpretation of upcoming policy or regulations and does not ask respondents to predict final compliance requirements resulting from this EO.

BACKGROUND AND PROBLEM STATEMENT

Defense supply chains are complex, distributed, and dependent on organizations and assets beyond the direct contractual relationship. An organization may have strong visibility into its direct suppliers while lacking consistent information about lower-tier sources to understand production locations, ownership and control, raw-material origins, software dependencies, capacity constraints, or concentration risk. Data may also be fragmented across enterprise systems, supplier portals, commercial datasets, program teams, and manual processes.

The challenge is not simply to collect more data. For supply chain visibility to be impactful and actionable, it must be designed around the decisions an organization needs to make. This means focusing on critical supply chain elements, collecting information at the appropriate depth and frequency, establishing confidence in the information, and balancing its value against the burden placed on participants. The resulting insights should help organizations identify exposure, prioritize risk, support alternate sourcing and qualification, track mitigation efforts, and monitor changes over time.

WORKING DEFINITION & SCOPE

For purposes of this RFI, MxD uses the following working definition of supply chain visibility for respondent reaction:

Supply chain visibility is the ability to identify, trace, and understand critical suppliers, sites, components, software, materials, services, relationships, dependencies, and relevant risk conditions across multiple tiers, with sufficient data quality and timeliness to support resilience decisions and mitigation actions.

Respondents are encouraged to challenge or refine this definition. Relevant scope may include:

- Supply-chain depth: direct suppliers through lower-tier suppliers, processors, service providers, logistics nodes, and sources of raw materials.
- Objects of visibility: organizations, facilities, products, systems, parts, components, software, materials, equipment, and services.
- Lifecycle coverage: design, sourcing, qualification, production, delivery, sustainment, repair, modernization, and end-of-life transitions.
- Decision uses: disruption response, risk assessment, vulnerability and concentration analysis, capacity planning, alternate-source qualification, compliance evidence, and mitigation tracking.

CAPABILITY AREAS OF INTEREST

MxD is interested in integrated approaches as well as focused capabilities that address one or more of the following areas:

- Multi-tier mapping and relationship discovery, including sub-tier supplier identification and raw-material or component traceability.
- Indentured bill-of-materials development and maintenance, including hardware, software, materials, and associated provenance.
- Assessment of financial, foreign ownership/control/influence, manufacturing and supply, cyber, geopolitical, counterfeit, logistics, capacity, obsolescence, and concentration risks.
- Identification of vulnerabilities, bottlenecks, sole-source or single-source dependencies, and other single points of failure.
- Risk prioritization, scenario analysis, alerts, corrective-action workflows, mitigation tracking, and closeout evidence.
- Data ingestion and interoperability across ERP, PLM, MES, QMS, procurement, logistics, supplier-portal, and external data sources.
- Secure and trusted data-sharing models that protect proprietary information, regulated data, intellectual property, and sensitive supplier relationships.
- Approaches that reduce reporting burden and enable participation by small and medium manufacturers, non-traditional defense firms, and new entrants.

RESPONDENT PROFILE

MxD welcomes responses from individual organizations or teams. Respondents do not need to address every capability area. Relevant respondents may include:

- Technology providers offering supply-chain mapping, traceability, risk intelligence, analytics, data exchange, enterprise integration, or workflow capabilities.
- Consulting, systems-integration, testing, assurance, qualification, and supplier-development organizations.
- Defense and aerospace primes, tiered suppliers, and manufacturers with implemented visibility practices or active use cases.
- Universities, research institutions, industry associations, standards organizations, data collaboratives, and public-sector organizations.
- Organizations in adjacent sectors with transferable practices, including automotive, energy, electronics, pharmaceuticals, semiconductors, and critical infrastructure.

INFORMATION REQUESTED

Please provide the following information:

- Company name and U.S. address
- U.S. based point of contact (email and phone number)
- Organization type, size or market segment, and relevant experience
- Summary of capabilities, products, services, research, or implemented practices
- Links or attachments of relevant product literature, architecture diagrams, or case studies

QUESTIONS FOR RESPONDENTS

A. Solution and capability overview

1. Describe your organization's relevant solution, capability, or approach to establishing or improving multi-tier supply chain visibility. What primary use cases and decisions does it support?
2. What aspects of supply chain visibility does your capability address (e.g., supplier discovery and mapping, multi-tier relationships, component or material traceability, risk identification, dependency analysis, monitoring, or mitigation)?

B. Technical approach and data

3. Describe your approach to discovering, mapping, and validating multi-tier supply chain relationships, including suppliers, production locations, components, software dependencies, and raw-material sources. Where applicable, describe how multi-level or indentured BOM information is created, incorporated, or maintained.
4. How do you identify and validate suppliers, facilities, parts, materials, and relationships across different data sources? How do you assess the completeness, timeliness, accuracy, provenance, and confidence of the resulting information?
5. What data sources, standards, and exchange formats does your approach use or support? How does it integrate with relevant enterprise, manufacturing, procurement, logistics, supplier, or external risk-data systems? Describe how it reconciles differences in terminology, classifications, and data structures across suppliers and systems.
6. Describe the technical or operating architecture, deployment options, and major prerequisites for implementation. How can the approach scale across programs, business units, supplier tiers, or organizations?

C. Risk and decision support

7. What types of supply chain risks, dependencies, or vulnerabilities can the approach identify or monitor? Describe how it identifies areas such as sole-source dependencies, bottlenecks, geographic or ownership concentrations, capacity or lead-time constraints, supplier financial health, or other single points of failure.
8. How are identified risks translated into actionable information or workflows? Describe any risk prioritization, scenario analysis, disruption modeling, or predictive capabilities and how uncertainty is communicated to users.
9. How does the approach support mitigation activities, such as alternate sourcing, supplier qualification, corrective actions, assignment of responsibility, and tracking mitigation through closure?

D. Governance, trust, and supplier adoption

10. What information is required from primes, suppliers, third parties, government sources, or public sources? Who owns or controls that information, and what information – if any – should not be centralized?
11. How does the approach protect proprietary, export-controlled, CUI, or other sensitive information when data is shared or analyzed across organizational boundaries?
12. What factors most commonly enable or prevent supplier participation? What approaches to onboarding, technical assistance, incentives, funding, or shared services have proven effective, particularly for small and medium manufacturers?
13. How can supply chain information requests be harmonized or reused across customers while allowing requirements to be tailored based on supplier criticality, tier, product type, or risk?

E. Implementation, evidence, and transferability

14. Describe the maturity of your capability or approach and provide relevant implementation examples. Where possible, include the problem addressed, scope, approach, outcomes, limitations, and lessons learned.
15. What organizational roles, skills, governance, and change-management practices are required to deploy, operate, and sustain the approach?
16. What measures or evidence demonstrate that the approach improves supply chain resilience or decision-making rather than simply increasing the amount of data collected? What important limitations or failure modes should be considered?
17. What practices or lessons from other industries could be applied to defense and aerospace supply chains? What defense-specific requirements or conditions would require those approaches to be adapted?

F. Ecosystem and pilot opportunities

18. Where could shared definitions, data models, reference architectures, services, test environments, implementation guidance, or other collaborative resources create the greatest value across the defense industrial ecosystem? Identify any significant capability, issue, or stakeholder not otherwise addressed by this RFI.
19. If MxD facilitated a pilot or demonstration, what narrowly scoped use case would generate useful evidence of value and feasibility? Identify the minimum participants, data, systems, supplier tiers, and governance arrangements required.
20. What outputs or decision criteria should be used to determine whether a pilot or approach is successful and suitable for broader adoption?

RESPONSE FORMAT AND LIMITS

Responses should be limited to five (5) pages of narrative. Supporting product literature, architecture diagrams, case studies, or standards references may be attached separately and are not counted toward this limit. Respondents are encouraged to address each question relevant to their capability and indicate “Not Applicable” where appropriate. Concise, bulleted responses are encouraged where appropriate.

- Submit one PDF named CompanyName_MxD_SupplyChainVisibility_RFI.pdf
- Clearly identify the question numbers addressed.
- Clearly and conspicuously mark proprietary or confidential information.
- Do not submit classified information, Controlled Unclassified Information, export-controlled technical data, or customer information that the respondent is not authorized to disclose.

SUBMISSION INSTRUCTIONS

Each respondent must submit their response no later than 8:00PM Central Time, September 4, 2026. All submissions must be submitted electronically to MxD’s submission form, [HERE](#).

Please complete the form and hit SUBMIT to fully submit your response.

DISCLAIMERS

This Request for Information is issued by MxD for planning and ecosystem discovery purposes only. It is not a solicitation, Request for Quotation, Request for Proposal, grant opportunity, or offer to contract. Issuance of this RFI does not obligate MxD to issue any follow-on opportunity or make any award.

Responses are not quotations, bids, or offers and will not be accepted or treated as such. Unless MxD separately states otherwise in a future notice, responses will not be scored or ranked for selection or used as the basis for an award.

Respondents bear all costs associated with preparing and submitting a response. MxD will not reimburse any cost incurred in responding to this RFI.

Submitting a response is not a prerequisite to participating in any future MxD activity or solicitation, and declining to respond will not disadvantage an organization in any future opportunity. Responding confers no preference, advantage, or right to participate.

Information received may be used by MxD to refine its understanding of the problem, identify ecosystem capabilities and gaps, shape potential research or pilot concepts, and inform future engagement. Respondents must not submit classified information or Controlled Unclassified Information. Proprietary or confidential information must be clearly and conspicuously marked.

MxD reserves the right to contact any respondent for clarification and may elect not to pursue any activity described or contemplated in this RFI.

References to Executive Order 14415 and potential future implementation requirements are provided solely as policy context. This RFI does not provide legal, regulatory, or contractual guidance.