



Critical Manufacturing Sector-Specific Plan

An Annex to the NIPP 2013

2015



Homeland
Security

TABLE OF CONTENTS

COORDINATION LETTER FROM COUNCIL CHAIRS	iii
EXECUTIVE SUMMARY	iv
1 INTRODUCTION	1
2 SECTOR OVERVIEW	2
2.1 Sector Profile	2
Key Sector Operating Characteristics	2
Sector Components and Assets	4
2.2 Sector Risks	5
Notable Trends and Emerging Sector Issues	5
Significant Critical Manufacturing Sector Risks	5
Primary Cross-Sector Interdependencies	6
2.3 Critical Infrastructure Partners	7
Critical Manufacturing Sector Partnership Structure	7
Value Proposition for Participation in the Sector Partnership	9
3 RISK MANAGEMENT AND NATIONAL PREPAREDNESS	10
3.1 Risk Management	10
Identify Infrastructure	10
Assess and Analyze Risks	11
Implement Risk Management Activities	11
3.2 Managing Cyber Risks	12
3.3 Mitigating Disruption from Loss of Lifeline Functions	12
3.4 Research and Development Priorities	13
3.5 Critical Manufacturing Sector National Preparedness Efforts	13
4 MISSION, GOALS, AND PRIORITIES	15
4.1 Critical Manufacturing Sector Activities	16
5 MEASURING EFFECTIVENESS	17
Appendix A Alignment with the NIPP 2013	20
Appendix B Geographic Concentration of Critical Manufacturing Facilities by Component	23

COORDINATION LETTER FROM COUNCIL CHAIRS

In 2008, the Secretary of the Department of Homeland Security established the Critical Manufacturing Sector, recognizing the sector's key resources and significant national impact.* Since then, the sector has successfully built public-private partnerships, improved information sharing, created forums to share best practices, and developed tools and exercises to improve incident response and recovery. The sector recognizes the value of the public-private partnership and continues to take steps to improve security and resilience.

2015 Sector-Specific Plan Update

This 2015 release of the Critical Manufacturing Sector-Specific Plan updates the original plan issued in 2010. As with the previous plan, this Sector-Specific Plan represents a collaborative effort among the private sector; Federal, State, local, tribal, and territorial governments; and nongovernmental organizations to reduce the risk to critical infrastructure.

The Critical Manufacturing Sector Coordinating Council and Government Coordinating Council jointly developed the goals, priorities, and activities included in this Sector-Specific Plan to reflect the overall strategic direction for the Critical Manufacturing Sector. The Sector's goals support the [Joint National Priorities](#) developed in 2014 by the national council structures described in the [National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience \(NIPP 2013\)](#).

This Sector-Specific Plan also illustrates the continued maturation of the Critical Manufacturing Sector partnership and the progress made to address the sector's evolving risk, operating, and policy environments.

Key Accomplishments

Since 2010, Critical Manufacturing Sector public and private sector partners have taken significant steps to reduce sector risk, improve coordination, and strengthen security and resilience capabilities:

- Gathered wide private sector input for the [National Strategy for Global Supply Chain Security](#).
- Developed supply chain resilience workshops to improve information exchange in support of the National Strategy.
- Developed a Business Continuity Plan Suite designed to help small- and mid-size businesses develop robust continuity plans and improve resilience along sector and cross-sector supply chains.
- Developed tabletop exercises specifically aligned with the emergency response plans of Sector Coordinating Council members, creating opportunities for stakeholders to discuss supply chain disruption and resilience practices, facility access control, and issues with disgruntled employees.
- Established the Global Crisis Response System to serve as a small community discussion forum in the event of an overseas crisis.

These achievements represent the effective and value-added collaboration of the Critical Manufacturing Sector Coordinating Council, Government Coordinating Council, and the U.S. Department of Homeland Security as the Sector-Specific Agency. They clearly demonstrate the sector's progress in working toward a rational approach to develop, prioritize, and implement effective security programs and resilience strategies.

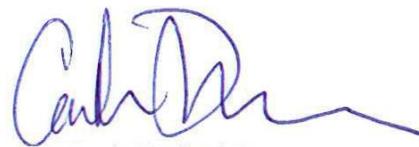
In the same shared purpose that guided these actions, Critical Manufacturing Sector partners look forward to continuing their efforts to enhance the security and resilience of our Nation's critical infrastructure assets.



Jason R. Rosselot

Chair

Critical Manufacturing
Sector Coordinating Council



Caitlin A. Durkovich

Assistant Secretary

Office of Infrastructure Protection
U.S. Department of Homeland Security
Chair, Critical Manufacturing Government Coordinating Council

* U.S. Department of Homeland Security, "Designation of the National Infrastructure Protection Plan Critical Manufacturing Sector," *Federal Register*. (April 30, 2008), <https://www.federalregister.gov/articles/2008/04/30/E8-9412/designation-of-the-national-infrastructure-protection-plan-critical-manufacturing-sector>.

EXECUTIVE SUMMARY

The Critical Manufacturing Sector includes the manufacturing industries that are the most crucial for the continuity of other critical sectors and have significant national economic implications. Manufacturers in the sector process raw materials and primary metals; produce engines, turbines, and power transmission equipment; produce electrical equipment and components; and manufacture cars, trucks, commercial ships, aircraft, rail cars, and their supporting components. A failure or disruption in the Critical Manufacturing Sector could result in cascading disruptions to other critical infrastructure sectors in multiple regions.†

Critical Manufacturing Sector Assets and Risks

Critical Manufacturing Sector assets are privately owned and operated and include manufacturing facilities, processing and distribution facilities, sales offices, corporate headquarters, and product storage. With facilities, vendors, suppliers, and customers located around the globe, the Critical Manufacturing Sector is vulnerable to a variety of risks, including natural disasters, terrorism, cyberattacks, and geopolitical unrest. Central to the sector's operations is the global transport of raw materials and finished products along large supply chains. Local or regional disruptions to critical suppliers can thus cascade across wide geographic regions and industries.

With rising international commerce, manufacturers' supply chains have grown more extensive, complex, and interdependent—involving potentially hundreds of suppliers in as many regions. A global web of transportation pathways, information technology, and cyber and energy networks have created supply chain efficiencies that enable just-in-time shipments and reduced inventories—but also decrease the ability to absorb disruptions.

Partnering to Improve Security and Resilience

When owners and operators better understand their risks and interdependencies, they can develop business continuity strategies that build agility and redundancy into supply networks and implement security practices that mitigate facility and asset risks. Each company is responsible for managing individual operational risks. Owners and operators conduct risk assessments for facilities, systems, and supply chains using a variety of methodologies, typically by working with its first tier vendors and customers and their second tier network of suppliers. Yet interdependencies among manufacturers and with other critical industries dictate that owners and operators cannot effectively evaluate and mitigate risks working alone.

The [National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience \(NIPP 2013\)](#) partnership structure enables owners and operators to work directly with their peers through the Sector Coordinating Council, and with Federal, State, local, tribal, and territorial partners through the Government Coordinating Council. Partners collaborate on a voluntary basis to share actionable, relevant risk information; exchange best practices; build cross-sector situational awareness; and enable risk-informed decision-making.

Through this partnership, the Critical Manufacturing Sector has developed tools, resources, and programs that support sector-wide risk management and maximize partners' limited resources. Key examples include tabletop exercises and training workshops focused on supply chain resilience and business continuity planning, an annual conference and road shows to exchange information and promote government security and resilience resources, classified threat briefings for cleared owners and operators, and a Global Crisis Response System that serves as a discussion forum for owners and operators during overseas crises.

2015 Sector-Specific Plan

This Critical Manufacturing Sector-Specific Plan is designed to guide the sector's voluntary, collaborative efforts to improve security and resilience during the next four years. It describes how the Critical Manufacturing Sector manages risks and contributes to national critical infrastructure security and resilience as set forth in [Presidential Policy Directive 21: Critical Infrastructure Security and Resilience](#). As an annex to the NIPP 2013, this Sector-Specific Plan tailors the strategic guidance provided in the NIPP 2013 to the unique operating conditions and risk landscape of the Critical Manufacturing Sector. As such, the sector strategy supports the NIPP 2013 national goals and strategy, the 2014 [Joint National Priorities](#), and implementation of [Executive Order 13636: Improving Critical Infrastructure Cybersecurity](#).

† U.S. Department of Homeland Security, "Designation of the National Infrastructure Protection Plan Critical Manufacturing Sector," Federal Register. (April 30, 2008), <https://www.federalregister.gov/articles/2008/04/30/E8-9412/designation-of-the-national-infrastructure-protection-plan-critical-manufacturing-sector>.

Sector Goals, Priorities, and Activities

As part of this 2015 Sector-Specific Plan, the Critical Manufacturing Sector Coordinating Council and Government Coordinating Council have identified goals and priorities to guide the sector's security and resilience efforts over the next four years and to address or mitigate the sector's risks.

The councils set four goals:

1. Improve information sharing and promote continuous learning.
2. Identify sector-specific risks.
3. Develop cost-effective strategies to reduce these risks.
4. Support research and development efforts and advanced planning to ensure rapid response and recovery.

To achieve these goals, the sector partners developed six priorities to focus their efforts. The priorities include evaluating interdependencies with other sectors and within their supply chains; increasing engagement and collaboration both within the sector and with other critical infrastructure sectors; raising risk awareness at executive levels; improving cybersecurity knowledge, tools, capabilities, and practices; and participating in cross-sector trainings and exercises to improve response and recovery.

Figure ES-1. Alignment of National and Sector-Specific Goals, Priorities, and Activities



As part of a detailed implementation plan, the sector identified 14 activities that sector partners plan to undertake, as resources allow, to improve the security and resilience of U.S. Critical Manufacturing Sector operations over the next one to four years. [Chapter 4](#) provides a detailed list of planned sector activities.

The Critical Manufacturing Sector aligned its Sector-Specific Plan with the national planning framework for security and resilience in the NIPP 2013. As a result, progress toward sector goals, priorities, and activities contributes directly to national achievements under the NIPP 2013. [Appendix A](#) demonstrates the detailed alignment of this Sector-Specific Plan to NIPP 2013 goals, the Joint National Priorities, and the NIPP 2013 Calls to Action.

1 INTRODUCTION

This 2015 *Critical Manufacturing Sector-Specific Plan* sets the strategic direction for voluntary, collaborative efforts to improve sector security and resilience over the next four years. It describes how the Critical Manufacturing Sector manages risks and contributes to national critical infrastructure security and resilience as set forth in [Presidential Policy Directive 21: Critical Infrastructure Security and Resilience](#). As an annex to the [National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience \(NIPP 2013\)](#), this Sector-Specific Plan tailors the strategic guidance provided in the NIPP 2013 to the unique operating conditions and risk landscape of the Critical Manufacturing Sector. As such, the sector strategy supports the NIPP 2013 national goals and strategy, the 2014 [Joint National Priorities](#), and implementation of [Executive Order 13636: Improving Critical Infrastructure Cybersecurity](#). Public and private sector representatives have identified shared goals and priorities and a supporting set of collaborative activities they plan to pursue during the next four years, as resources allow.

Sector-Specific Plan development answers NIPP 2013 Call to Action #2, which requires each of the [16 designated critical infrastructure sectors](#) to update their Sector-Specific Plan every four years to reflect joint priorities, address sector reliance on lifeline functions, describe national preparedness efforts, outline cybersecurity efforts, and develop metrics to measure progress. [Appendix A](#) illustrates how the Critical Manufacturing Sector's goals, priorities, and activities support the NIPP 2013 national goals, the five Joint National Priorities developed in 2014 collaboratively by industry and government in accordance with the NIPP 2013, and other Calls to Action.

This plan describes the Critical Manufacturing Sector's approach to risk management and national preparedness—considering its distinct assets, operations, and risk profile—in support of Federal plans and directives for security and resilience. The remainder of this Critical Manufacturing Sector-Specific Plan includes:

- [Chapter 2: Sector Overview](#)—Provides a view of the sector's assets and operating characteristics, risk profile, and key public and private sector partners.
- [Chapter 3: Risk Management and National Preparedness](#)—Describes the mechanisms to achieve sector goals, including ongoing and planned partnership programs, activities, and resources that support the sector's current risk management approach; research and development priorities; and how the sector supports national preparedness through incident response and recovery.
- [Chapter 4: Mission, Goals, and Priorities](#)—Presents the sector's mission, updated goals and priorities for Critical Manufacturing Sector security and resilience for the next four years, and the specific activities that the Critical Manufacturing Sector public and private sector stakeholders plan to conduct.
- [Chapter 5: Measuring Effectiveness](#)—Describes the planned approach to measure the effectiveness of individual activities and report on sector progress.

This Sector-Specific Plan provides targets for collaborative planning among the U.S. Department of Homeland Security, as the Sector-Specific Agency, and the Critical Manufacturing Sector Coordinating Council and Government Coordinating Council members. Partners have a clear and shared interest in ensuring the security and resilience of critical sector assets, systems, and networks, and this plan represents the voluntary, collaborative activities that could greatly reduce sector risk and build resilience during the next four years.

2 SECTOR OVERVIEW

This chapter profiles the Critical Manufacturing Sector’s assets, design, and operating characteristics; identifies its primary risks and interdependencies; and describes how the sector’s public-private partnership operates.

2.1 Sector Profile

The Critical Manufacturing Sector processes raw materials and produces highly specialized parts and equipment that are essential to primary operations in several U.S. industries—particularly transportation, defense, electricity, and major construction. In 2013, the U.S. manufacturing industry contributed \$2.08 trillion to the economy, representing 12.5 percent of the Gross Domestic Product. On its own, manufacturing in the United States would be the eighth-largest economy in the world.¹

Critical Manufacturing Sector products form the backbone of energy and transportation infrastructure in the United States. Many Critical Manufacturing Sector facilities also produce key elements or products for defense and are a part of the Defense Industrial Base Sector. A major failure or disruption in the sector could result in significant national economic impact and lengthy disruptions that cascade across multiple critical infrastructure sectors or regions. This Sector Profile describes key characteristics of the Critical Manufacturing Sector that influence its security and resilience.

Key Sector Operating Characteristics



Most manufacturing enterprises are integrated into complex, interdependent global supply chains.

Nearly all manufacturers are part of a chain of suppliers, vendors, partners, integrators, contractors, and customers that link to other industries and businesses. The level of supply chain resilience influences each firm’s risks and competitiveness, requiring companies to work closely with supplier and customer networks to improve reliability.



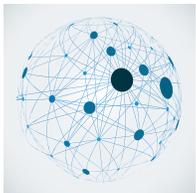
An uninterrupted supply of energy and water is needed for high-temperature and power-intensive operations.

Although all businesses depend on energy and water, manufacturers typically require these resources in large amounts and in constant supply—particularly natural gas and electricity. As a result, disruptions in these critical sectors can rapidly cascade to Critical Manufacturing Sector operations.



Geographic concentration localizes expertise and reduces logistics costs.

Critical Manufacturing Sector facilities are heavily clustered around major U.S. coastal ports. This not only allows for the easy delivery of raw materials imports and international product distribution, but also subjects multiple producers to local and regional disruptions. Global supply networks may also converge in strategic geographic areas—whether by rarity of materials or concentrated production capabilities—which creates pinch points that can magnify disruptions.



The sector’s global networks demand constant monitoring to anticipate and mitigate disruptions.

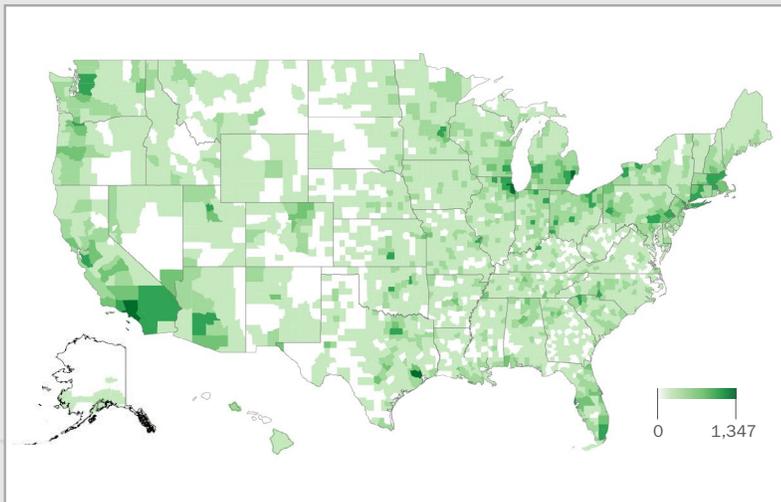
The Critical Manufacturing Sector includes facilities, employees, suppliers, and customers around the world. Complex international networks of raw materials and finished products expose U.S. operations to a range of global risks and geopolitical conditions.

CRITICAL MANUFACTURING SECTOR SNAPSHOT

<p>Primary Metals</p> <p>Processes aluminum, iron, and steel that supports transportation, urban centers, energy supply, clean water, safe food, and defense.</p> 	<p>Machinery</p> <p>Manufactures engines, turbines, power-transmission equipment, and heavy machinery.</p> 	<p>Electrical Equipment, Appliance, & Component</p> <p>Manufactures specialized power generation equipment, including critical transformers and generators.</p> 	<p>Transportation</p> <p>Manufactures critical components for cars, trucks, commercial ships, commercial aircraft, and rail parts for both passenger and freight.</p> 
--	---	---	--

INFRASTRUCTURE CHARACTERISTICS

Location of U.S. Critical Manufacturing Facilities by County



Map developed using data from: U.S. Census Bureau, "Economic Census: Industry Snapshots 2012," NAICS codes 331, 333, 335, 336, last revised February 28, 2012, <http://www.census.gov/econ/snapshots/index.php>.

†† National Association of Manufacturing, "Facts About Manufacturing," accessed November 25, 2014, <http://www.nam.org/Statistics-And-Data/Facts-About-Manufacturing/Landing.aspx>.

* Rosselot, Jason, "Partnership for More Secure Manufacturing," Panel: Industrial Cyber Security, (Critical Manufacturing Sector Coordinating Council, April 2015).

Manufacturing facilities are geographically concentrated around coastal ports, positioned for massive importing and exporting of materials and products. This may magnify geographic risks and the effects of local disasters.

60% of U.S. exports are produced by the manufacturing industry.^{††}

Global supply chains have grown longer and more complex—increasing susceptibility to a range of global hazards, but improving production agility.

Supply chains focus on efficiency, not redundancy. Lean inventories and just-in-time practices increase vulnerability to long-term disruptions.

Supply chain disruptions are one of the top five security concerns cited by Critical Manufacturing Sector Coordinating Council members.*

CRITICAL SECTOR INTERDEPENDENCIES

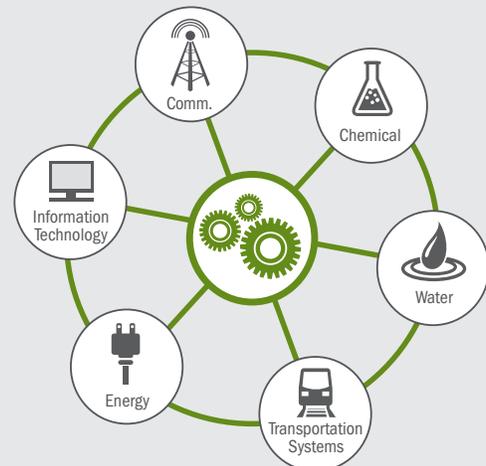
Manufacturing—Manufacturers process raw material and produce specialized equipment for other manufacturing operations.

Energy and Water—Essential manufacturing operations require large, uninterrupted supplies of energy and water.

Communications and IT—Communications networks and IT systems underpin supply chain coordination and control system processes.

Transportation Systems—Multiple modes enable the global movement of large and specialized products.

Chemical—Processes require regular supply of a range of chemical products.



Sector Components and Assets

The Critical Manufacturing Sector represents a range of manufacturers that differ based on function, size, operating principles, and security risks. The sector is grouped into four component areas as defined in the Federal Register, based on similar functions and operations. The private sector owns and operates the vast majority of U.S. Critical Manufacturing Sector infrastructure—46,259 establishments as of February 2012.² Key assets, systems, and networks in each component area include manufacturing facilities, processing and distribution facilities, sales offices, corporate headquarters, and product storage. [Appendix B](#) illustrates the geographic concentration of facilities in the sector.

Primary Metals Manufacturing



Iron and Steel Mills & Ferro-alloy Manufacturing



Alumina and Aluminum Production & Processing



Non-ferrous Metal Production & Processing

Primary metals manufacturers convert raw materials into assemblies, intermediate products, and end products. These products can include sheet metal, bar stock, I-beams, slabs, or pipes. The 4,556 manufacturers in this component area were responsible for \$270.9 billion in U.S. shipments in 2012.³

Machinery Manufacturing



Engine & Turbine Manufacturing



Power-Transmission Equipment Manufacturing



Earth Moving, Mining, Agricultural, & Construction Equipment

Machinery manufacturers produce engines, turbines, and power-transmission equipment. These large, specialized products support infrastructure and primary operations in a number of critical U.S. industries. Heavy-equipment manufacturers produce equipment used in earth moving, mining, agriculture, and construction, as well as other heavy-material handling equipment. The 24,124 manufacturers in this component area were responsible for \$407.6 billion in U.S. shipments in 2012.⁴

Electrical Equipment, Appliance, and Component Manufacturing



Electric Motor Manufacturing



Transformer Manufacturing



Generator Manufacturing

Electrical equipment manufacturers produce specialized equipment, assemblies, intermediate products, and end products for power generation. These products can include transformers, electric motors and generators, and industrial controls. The 5,765 manufacturers in this component area were responsible for \$123.9 billion in U.S. shipments in 2012.⁵

Transportation Manufacturing



Vehicles & Commercial Ships



Aerospace Products & Parts



Locomotives, Railroad and Transit Cars, & Rail Track Equipment

Transportation manufacturers produce cars and trucks, aircraft and component parts, aerospace products and parts, railroad cars and other railroad products, and other transportation equipment. The 11,814 manufacturers in this component area were responsible for \$792.9 billion in U.S. shipments in 2012.⁶

2.2 Sector Risks

Successful risk management for the Critical Manufacturing Sector depends on the ability of owners and operators to continuously monitor and analyze evolving threats, swiftly identify and mitigate static and emerging vulnerabilities, and thoroughly understand potential consequences of a disruptive event. This section identifies emerging issues that may exacerbate risks to the Critical Manufacturing Sector and provides an overview of the sector's risk profile.

Notable Trends and Emerging Sector Issues

- **Supply chains have been optimized for productivity and efficiency.** Maintaining low material and product inventories and eliminating redundant suppliers creates efficient, cost-effective supply chains. These lean supply and delivery networks can increase vulnerability to cascading disruptions and decrease agility in response with potentially damaging financial implications. Companies must balance optimization that effectively mitigates recurring risks with resilience strategies needed to withstand infrequent, yet high-impact risks.
- **Globalization and outsourcing have linked U.S. manufacturers with foreign suppliers, vendors, and customers through highly interdependent supply networks.** Manufacturers have increasingly turned to foreign markets for raw materials, component manufacturing, equipment and machinery, labor, and customers as a way to reduce overall costs. This increased dependence on international networks subjects the sector to a range of global risks.

Significant Critical Manufacturing Sector Risks

Natural Disasters and Extreme Weather



Increasingly extreme weather events and natural disasters increase the vulnerability of facilities and employees in certain geographic regions. Yet the sector's assets, suppliers, and customers are dispersed globally, making operations susceptible to natural disasters across the globe that can trigger cascading disruptions in affected supply chains. Disasters can also interrupt critical Energy, Water, and Transportation Systems Sector services and cause delays or manufacturing shutdowns.

Supply Chain Disruptions



Incredibly efficient supply chains have resulted in a "just-in-time" delivery model that leaves companies with very limited inventories, making some manufacturers highly sensitive to substantial and cascading economic consequences. Operations may be disrupted if raw materials are unable to reach company facilities in a timely manner. Similarly, manufacturers may face significant economic consequences if they cannot deliver finished products to customers on time. Shipment tracking and management, in particular, may rely on the Global Positioning System and its precise positioning, navigation, and timing data. A disruption in these data could create cascading supply chain disruptions.

Global Political and Social Implications



The Critical Manufacturing Sector's global network requires manufacturers to closely monitor geopolitical unrest, global attitudes toward the United States, radicalism, economic conditions, and other risk factors. Such variables may affect foreign operations, supply chain partners, or materials sources and trigger cascading disruptions that affect U.S. companies and commerce.

Deliberate Attacks and Terrorism



The economic, strategic, and iconic value of the sector may make it an attractive target for terrorists who aim to destroy facilities or interfere with manufacturing operations. An attack on a Critical Manufacturing Sector facility by extremist groups or international terrorist organizations could cause mass casualties and draw extensive media attention.

Cyberattacks



Manufacturing processes are typically operated by industrial control systems that increasingly use open platforms and common operating systems, rather than proprietary system designs. Cyber intruders may aim to seize control of the systems to disrupt processes, corrupt information sent to facility operators, damage equipment, or steal proprietary information. Intellectual property theft through cyberattacks can threaten competitiveness, affect business reputation, and subject customers to risk from counterfeit products. Intellectual property shared with business partners outside the company also becomes subject to the security risk of partners' systems.

Primary Cross-Sector Interdependencies

Critical Manufacturing Sector operations are closely integrated with other critical sector services, which creates interdependencies that can cause a disruption in one sector to affect operations in another. Local disasters can cascade to multiple jurisdictions and sectors, triggering damage across larger geographic areas. Limited visibility into growing risks faced by interdependent sectors may subject manufacturers to “hidden risks”—spillover risks from other sectors that Critical Manufacturing Sector owners and operators cannot adequately anticipate or manage.

The NIPP 2013 identifies lifeline functions—energy, water, communications, and transportation systems—as services and resources that are essential to the operations of most critical infrastructure partners and communities. Identifying lifeline functions, specifically those that are interdependent with other sectors, can help owners and operators prepare for and mitigate the loss of these services in an emergency. In the Critical Manufacturing Sector, transportation systems provide lifeline functions and are also essential to the supply chain. Although the Critical Manufacturing Sector may be interdependent in some way with all 16 critical infrastructure sectors, its most significant sector interdependencies include:

Internal: Manufacturing



Manufacturing operations, both commercial and defense, require processed materials, complicated machinery, and specialized equipment that are often manufactured by other firms in multiple component areas within the sector. For example, the intermediate and end products of Primary Metals Manufacturing may be required to manufacture end products in the Machinery Manufacturing component, and vice versa.

Lifeline Functions: Energy, Water, and Communications



Manufacturers require large amounts of uninterrupted power for operations. Although backup generation provides power needed to operate during short-term disruptions to safely shutdown a facility, a long-term outage would significantly disrupt operations.



In some cases, continuous water sources are essential for manufacturing processes. Manufacturers may have alternate sources of water available for short-term service interruptions, but a long-term outage could result in a significant shutdown.



Communications networks underpin the coordination of supply chain movements and control system processes. Owners and operators rely on the Communications Sector for telecommunications access for operations and logistics. The Critical Manufacturing Sector also relies on Communications Sector services for emergency notification and response.

Supply Chain Functions: Transportation Systems, Information Technology, and Chemical



The Transportation Systems Sector—also a lifeline function—enables the global movement of large and specialized materials and products on strict time lines. Manufacturers depend on multiple modes of transportation (aviation, freight rail, highway, and maritime) for the secure movement of raw materials and finished products—key components of their operations. The sector is at risk of piracy of shipping vessels, limited availability of rail lines due to increased overseas demand, potential labor disputes, and ports operating at maximum capacity. Major disruptions to transportation networks can overload other modes of transport as manufacturers seek alternatives to continue operations.



Critical Manufacturing Sector facilities rely heavily on information technology for their manufacturing operations, global transit, quality control systems, critical processes, and facility security. An information technology disruption in the Critical Manufacturing Sector would affect both production and distribution of sector products. As cyberattacks increase, manufacturers are also concerned about intellectual property theft and control system process disruption.



A consistent supply of a range of chemicals is required in multiple manufacturing sector processes. A disruption or delay in the chemical supply could create a cascading effect on production in the Critical Manufacturing Sector.

2.3 Critical Infrastructure Partners

Voluntary collaboration between private sector and government stakeholders has been—and remains—the primary mechanism for advancing collective action toward Critical Manufacturing Sector security and resilience. Like all 16 critical infrastructure sectors, the Critical Manufacturing Sector operates under the NIPP 2013 partnership structure, which encourages participation from the private sector; government partners at Federal, State, local, tribal, and territorial levels; and academic and nongovernmental organizations that support sector security and resilience.

Critical Manufacturing Sector Partnership Structure

Figure 1. Critical Manufacturing Sector Partnership Structure



The success of the Critical Manufacturing Sector partnership depends on the sector's success in leveraging the full spectrum of capabilities, expertise, and experience across the critical infrastructure community and associated stakeholders. The partnership is most effective when partners can efficiently share actionable, timely, and relevant information to build situational awareness and enable risk-informed decision-making.

The NIPP 2013 partnership structure employs representative public and private sector councils that operate under the Critical Infrastructure Partnership Advisory Council construct. This construct facilitates interaction between the community of owners and operators and the sector's Federal, State, local, tribal, and territorial government representatives to conduct deliberations and form consensus positions for the Federal Government.

Partnership councils meet to exchange ideas and lessons learned, facilitate sector-level planning and resource allocation, establish effective coordinating structures, and develop security and resilience tools, guidelines, products, and programs. They also work with coordinating councils in the other 15 critical infrastructure sectors and other advisory councils—including the State, Local, Tribal, and Territorial Government Coordinating Council and the Regional Consortium Coordinating Council—to collaborate on cross-sector and cross-jurisdictional security and resilience issues.

Critical Manufacturing Sector-Specific Agency

The U.S. Department of Homeland Security was designated as the Sector-Specific Agency, and serves as the lead coordinator of partnership activities and the primary Federal interface for sector-specific security and resilience. The Sector-Specific Agency promotes sector-wide information sharing and supports implementation of the NIPP 2013 within the Critical Manufacturing Sector.

The Office of Infrastructure Protection fulfills the role of Sector-Specific Agency on behalf of the U.S. Department of Homeland Security. The Assistant Secretary for Infrastructure Protection chairs the Critical Manufacturing Government Coordinating Council and has designated the Director of the Sector Outreach and Programs Division as the representative on behalf of the Office of Infrastructure Protection. The Director may designate an alternate to assist as necessary.

Critical Manufacturing Sector Coordinating Council

The Sector Coordinating Council is a self-organized, self-governed council of representatives from more than 60 manufacturing companies, including several large international manufacturers from each of the component areas. The council provides a forum for private companies to coordinate on sector strategy, policy, information sharing, and risk management activities. Members also use their networks and industry organizations to share information, resources, tools, and best practices developed by the councils. An up-to-date list of Critical Manufacturing Sector Coordinating Council member companies can be found on the [Critical Manufacturing Sector Charter and Membership Webpage](#).

Critical Manufacturing Government Coordinating Council

The Government Coordinating Council enables coordination and communication on Critical Manufacturing Sector security and security-related strategies, activities, and policies across and between Federal, State, local, tribal, and territorial government agencies. The Government Coordinating Council works closely with the Sector Coordinating Council to plan, implement, and execute sector-wide resilience and security programs for the Nation's Critical Manufacturing Sector facilities and community.

The Government Coordinating Council membership includes components within the U.S. Department of Homeland Security. All members participate in required meetings and planning sessions with the added responsibility of providing metrics associated with activities. Representatives from other departments and agencies are welcomed and encouraged to participate in Critical Manufacturing Government Coordinating Council meetings and provide relevant institutional knowledge and expertise.

Joint Council Working Groups

The Critical Manufacturing Sector establishes working groups when substantial investigation, research, or other tasks are required which cannot be achieved during regular council meetings. All Government Coordinating Council and Sector Coordinating Council members may designate individuals to serve on working groups, and new working groups may be formed at any time. Current joint working groups and collaboration mechanisms include:

- **Information and Intelligence Working Group:** Develops information needs for the sector and identifies information-sharing mechanisms.
- **Cybersecurity Working Group:** Assesses the sector’s cyber-risk landscape and identifies and prioritizes risk reduction activities.
- **Global Crisis Response System:** Provides a way for manufacturers to share information during an event and coordinate response to global incidents.
- **Region-Specific Councils:** Provide a venue for national-level Sector Coordinating Council members to come together and discuss region-specific risks and needs.

Value Proposition for Participation in the Sector Partnership

Critical Manufacturing Sector Coordinating Council members that actively participate in the sector partnership receive valuable benefits, including:

- Information exchange with the Federal Government.
- Improved access to actionable, timely, and accurate threat information.
- Exercises, training, tools, resources, and working groups tailored to meet companies’ physical security and cybersecurity needs.
- Networking opportunities and sharing of best practices between the private sector and government and within the private sector.

The benefits of participating in the public-private partnership improve partners’ situational awareness and understanding of sector risks, enabling members to more effectively:

- Minimize service disruption to ensure consistent, predictable revenue flow.
- Improve resilience and speed restoration of disrupted services.
- Raise public recognition for preparedness, continuity of service, and good corporate citizenship to maintain and enhance corporate reputations with investors, customers, and potential employees.

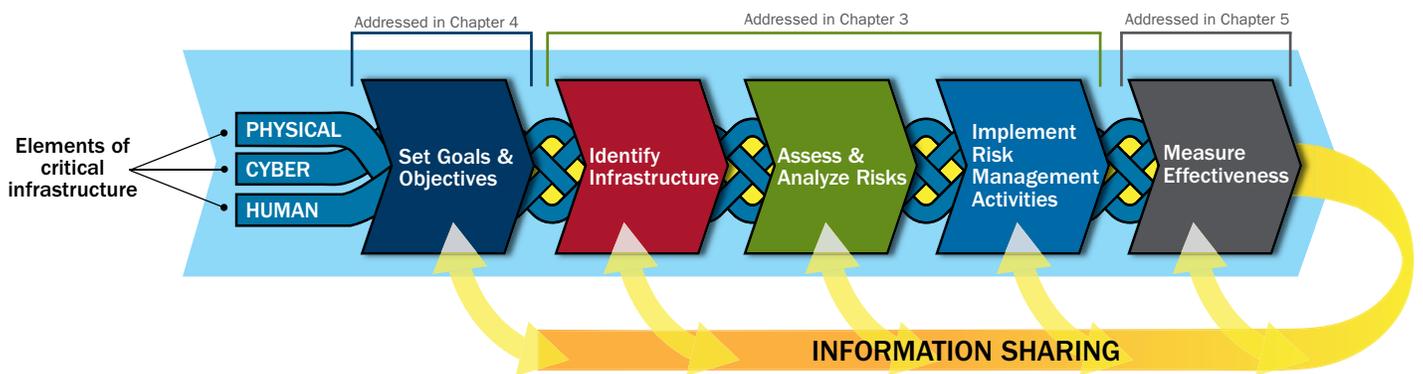
CHAPTER ENDNOTES

1. National Association of Manufacturing, “Facts About Manufacturing,” accessed September 14, 2015, <http://www.nam.org/Newsroom/Facts-About-Manufacturing/>.
2. U.S. Census Bureau, “Economic Census: Industry Snapshots 2012,” NAICS codes 331, 333, 335, 336, last revised February 28, 2012, <http://www.census.gov/econ/snapshots/>.
3. U.S. Census Bureau, “Economic Census: Industry Snapshots: Primary Metal Manufacturing (NAIC 331),” HR2 Econ Report Page, last revised April 23, 2015, http://thedataweb.rm.census.gov/TheDataWeb_HotReport2/econsnapshot/2012/snapshot.html?NAICS=331.
4. U.S. Census Bureau, “Economic Census: Industry Snapshots: Machinery Manufacturing (NAIC 333),” HR2 Econ Report Page, last revised April 23, 2015, http://thedataweb.rm.census.gov/TheDataWeb_HotReport2/econsnapshot/2012/snapshot.html?NAICS=333.
5. U.S. Census Bureau, “Economic Census: Industry Snapshots: Electrical Equipment, Appliance, and Component Manufacturing (NAICS 335),” HR2 Econ Report Page, last revised April 23, 2015, http://thedataweb.rm.census.gov/TheDataWeb_HotReport2/econsnapshot/2012/snapshot.html?NAICS=335.
6. U.S. Census Bureau, “Economic Census: Industry Snapshots: Transportation Equipment Manufacturing (NAICS 336),” HR2 Economic Report, last revised February 28, 2012, http://thedataweb.rm.census.gov/TheDataWeb_HotReport2/econsnapshot/2012/snapshot.html?NAICS=336.

3 RISK MANAGEMENT AND NATIONAL PREPAREDNESS

The NIPP 2013 uses risk management as the cornerstone of the national effort to strengthen security and resilience. It focuses on enabling owners and operators to make risk-informed decisions that best allocate limited resources. The critical infrastructure risk management framework—outlined in the NIPP 2013—enables the critical infrastructure community to focus on the threats and hazards most likely to cause harm and employs prioritized approaches designed to prevent or mitigate the effects of those threats and hazards. This approach also increases security and strengthens resilience by identifying and prioritizing actions to ensure continuity of essential functions and services during incidents and support rapid response and restoration on a continual basis.

Figure 2. NIPP 2013 Critical Infrastructure Risk Management Framework



The Critical Manufacturing Sector goals and priorities are rooted in the NIPP 2013 risk management framework. Updated goals and priorities reflect the maturation of the partnership and the significant progress made since the 2010 Sector-Specific Plan. This chapter presents the Critical Manufacturing Sector’s ongoing efforts and planned approaches to support risk management, national preparedness, and response and recovery following an incident that affects sector operations.

3.1 Risk Management

The NIPP 2013 defines risk as the potential for an adverse outcome from an event, determined by the event’s likelihood—a function of the specific threats and vulnerabilities—and associated consequences if the event occurs.⁷ Although owners and operators are responsible for managing risk to their individual assets, Critical Manufacturing Sector partnership activities can improve understanding of threats, vulnerabilities, and consequences and provide owners and operators with tools, guidelines, information, best practices, and resources to facilitate more effective risk assessments and risk management decisions at the facility and sector level.

Although there is no formal sector-wide approach for risk management in the Critical Manufacturing Sector, each company identifies its specific risks and structures within its business operations to minimize those risks, such as mapping supply chains, identifying redundant networks, and developing business continuity plans. The Critical Manufacturing Sector partnership aims to enhance the effectiveness of individual partner efforts by combining resources and expertise to enable more effective risk management. The following sections outline the sector’s approach to identifying infrastructure, assessing and analyzing risks, and implementing risk management activities, aligned with the NIPP 2013 risk management framework.

➤ Identify Infrastructure

The Critical Manufacturing Sector is distinct because its four component areas have already been identified as particularly critical to the U.S. manufacturing industry by the Federal Government.⁸ Owners and operators work with Federal, State, and local partners and members of other critical infrastructure sectors, such as Energy and Transportation Systems, to identify critical assets or operations. After identifying vital assets, owners and operators work with their partners to ensure that response and restoration activities for these assets are included in State, local, and regional response plans. Critical

Manufacturing Sector owners and operators also work with their critical customers and suppliers to develop emergency operations plans that identify contingencies and prioritize recovery of Critical Manufacturing Sector operations.

Assess and Analyze Risks

Individual sector owners and operators perform risk assessments for their critical assets. Due to the diversity of the Critical Manufacturing Sector, specific risk assessment methodologies may vary, from failure modes and effects analyses, to hazard and operability studies. These methodologies are used to determine risk to specific facilities, systems, supply chains, or other discrete components of the sector's infrastructure. The international scope of the sector's assets, networks, and products mean Critical Manufacturing Sector companies have extensive experience and sophisticated methodologies to analyze risks across global supply chains. These methodologies have also highlighted the importance of interdependencies within the Critical Manufacturing Sector and among the other critical infrastructure sectors.

To support individual company efforts to analyze risks and identify interdependencies, Critical Manufacturing Sector partners work to employ a variety of mechanisms to better identify and communicate threats, assess vulnerabilities, and evaluate consequences to form a more accurate picture of the risk environment:

- **Classified threat briefings from Federal agencies** provide the opportunity for appropriately cleared members of the sector to access classified intelligence products. Through these briefings, the sector is also able to provide feedback on the intelligence reports they receive, ensuring future reports better meet partners' intelligence needs. For example, private sector partners would like to receive an increased amount of raw intelligence data that may be more timely and actionable for owners and operators.
- **Tabletop exercises** hosted by Critical Manufacturing Sector partners also allow owners and operators to test their business continuity and resilience plans, build relationships with State and local governments, and gain insights into interdependencies that help determine what, if any, changes should be made to plans. The Critical Manufacturing Sector expresses a continued desire to use tabletop exercises to identify gaps in security and opportunities to improve resilience.
- The U.S. Department of Homeland Security assists partners in conducting **vulnerability assessments** to develop awareness of a facility's physical vulnerabilities and the connectivity, interdependencies, and weaknesses of operations and systems.
- The U.S. Department of Homeland Security offers **cyber assessments, evaluations, and reviews** to assist critical infrastructure sectors in identifying, prioritizing, and managing their cyber-infrastructure risk.

Implement Risk Management Activities

Critical Manufacturing Sector owners and operators conduct a number of activities to mitigate and manage risk, including implementing employee policies to protect against insider threat, assessing international operations, applying security practices across their enterprise, and purchasing adequate insurance. In addition to individual security practices and risk-mitigation measures implemented at individual facilities, owners and operators work with their peer companies and government partners to develop programs and conduct activities that help identify risks, prioritize resource investments, and improve knowledge and capabilities for risk management. The Critical Manufacturing Sector actively participates in risk management activities that include:

- **National-level exercises** to test sector and individual company plans.
- **Topic-specific working groups** to exchange information, discuss needs, and develop plans to address identified needs.
- Annual **road shows** to inform partners about available government resources for enhancing their security and resilience, conduct unclassified security briefings on cybersecurity, and hold high-level classified and unclassified briefings.
- **Tabletop exercises** specifically aligned with Sector Coordinating Council members' emergency response plans, creating opportunities for discussion among stakeholders concerning the supply chain, facility access control, and issues with disgruntled employees.
- **After-action reports** following sector exercises and security incidents to identify key areas for improvements.

- Annual **Critical Manufacturing Sector Security Conference** to provide a forum for partners to exchange information and gain an understanding of threats and vulnerabilities to their assets, systems, and networks.
- Private sector support for and implementation of the [National Strategy for Global Supply Chain Security](#).
- **Global Crisis Response System** to serve as a discussion forum for owners and operators to share information and coordinate response efforts during an overseas crisis that affects sector operations.
- **Supply chain resilience workshops** delivered nationally since April 2014 to share information and best practices from sector peers on resilience strategies and tools that address high-priority issues, including climate change adaptation, cybersecurity, and intellectual property theft.

3.2 Managing Cyber Risks

Cybersecurity risks and trends, when taken collectively, reach levels of scope and complexity that fall beyond the ability of individual industry and government organizations to manage. For example, when multiple organizations in an industry use the same software platform, they become vulnerable to the same exploits. Although organizations typically manage these types of issues on an individual basis or with a few key partners, examining risks from a sector level can provide significant long-term benefits. Working together, organizations can play an active role in identifying shared risks or those that threaten the viability or sustainability of the industry's products, services, or functions. The Critical Manufacturing Sector takes a collaborative approach to cyber risk by working with the U.S. Department of Homeland Security Office of Cybersecurity and Communication to evaluate the cybersecurity threats, vulnerabilities, and consequences of these critical functions to establish the sector's cyber risk management priorities.

The sector's cyber risk assessment and prioritization process builds on additional partnership activities to address cybersecurity:

- **The Critical Manufacturing Sector works closely with the Office of Cybersecurity and Communications** to support the Critical Infrastructure Cyber Community (C³) Voluntary Program, which is the coordination point within the Federal Government for critical infrastructure owners and operators interested in improving their cyber risk management processes. The program supports critical manufacturers in increasing the sector's cyber resilience and the sector's awareness and use of the National Institute of Standards and Technology [Framework for Improving Critical Infrastructure Cybersecurity](#). The Critical Manufacturing Sector leverages these programs to manage cybersecurity as part of an all-hazards approach to enterprise risk management.
- The Critical Manufacturing Sector-Specific Agency identified its critical cybersecurity functions and services as part of the **Cyber-Dependent Infrastructure Identification effort**. This effort identified sector critical functions that were validated by industry subject matter experts. As a result, the Critical Manufacturing Sector is positioned to conduct a sector-wide cyber-risk assessment leveraging the critical functions and services identified through the effort.

Once risks are validated, the sector will have a function-by-function view of cyber risk that will inform sector-specific risk management strategies and decision-making. This unified strategy provides the key linkage between national- and organization-level cyber risk management efforts. This enables the sector to take a risk-informed approach to its cybersecurity planning.

3.3 Mitigating Disruption from Loss of Lifeline Functions

Critical Manufacturing Sector owners and operators develop contingency plans, backup power and water sources, and alternate communication methods and transportation routes as part of their emergency operations and business continuity planning. In particular, owners and operators draw upon lessons learned from cross-sector partners during State and local emergency exercises to form more accurate expectations of lifeline function availability during a major disaster.

3.4 Research and Development Priorities

Research and development activities are critical for developing novel technologies and methods to better assess and mitigate risks to Critical Manufacturing Sector assets, systems, and networks. There are many cross-cutting research and development efforts, not only within the U.S. Department of Homeland Security, but also within Federal agencies, academia, and international initiatives. As the Critical Manufacturing Sector-Specific Agency, the U.S. Department of Homeland Security informs private sector partners of the latest developments in the sector's research and development portfolio.

Critical Manufacturing Sector owners and operators may also identify areas where they pursue research and development efforts individually or with private sector partners. The U.S. manufacturing industry is responsible for more than three-quarters of private sector research and development.⁹

As part of the NIPP 2013 partnership structure, critical infrastructure sectors identify research and development priorities that require the resources and expertise of both public and private sector partners. Cross-sector research and development priority areas were identified in the 2015 [National Critical Infrastructure Security and Resilience Research and Development Plan](#) and include:

- Develop the foundational understanding of critical infrastructure systems and systems dynamics.
- Develop integrated and scalable risk assessment and risk management approaches.
- Develop integrated and proactive capabilities, technologies, and methods to support secure and resilient infrastructure.
- Harness the power of data sciences to create unified, integrated situational awareness and to understand consequences of action.
- Build a crosscutting culture of critical infrastructure security and resilience research and development collaboration.

The Critical Manufacturing Sector plans to work closely with its Federal partners as part of plan implementation.

3.5 Critical Manufacturing Sector National Preparedness Efforts

Presidential Policy Directive 8: National Preparedness affirmed that preparation for major threats is a shared responsibility of all levels of government and the private and nonprofit sectors. It called for a National Preparedness System to help align the efforts of all partners for prevention, protection, mitigation, response, and recovery. [Section 3.1](#) provided an overview of the sector's key approaches to disaster prevention, protection, and risk mitigation. The sector also comprehensively prepares for effective sector response and recovery that supports the resilience of critical sector operations and regional and national resilience as a whole.

With extensive global supply chains that are sensitive to disruption, Critical Manufacturing Sector owners and operators have considerable experience with incident response and have repeatedly tested and refined their emergency action plans and business continuity plans under real-world conditions. They also work with their critical customers to ensure the availability of Critical Manufacturing Sector products and resources that support repairs and rapid restoration in the Energy and Transportation Systems Sectors.

Despite the potential large-scale implications of a major disaster, critical infrastructure preparedness, response, and recovery takes place primarily at the community and regional level among cross-sector owners and operators of regionally critical assets. Sector partners have conducted activities to improve incident response and recovery at the regional level to contribute to national preparedness, including:

- Partnered with the **Transportation Security Administration Highway and Motor Carrier Division** on supply chain exercises focused on natural disasters, information technology, cybersecurity, closed border crossings, and terrorist activities.

- Developed the **Business Continuity Planning Suite** of training, automated templates, and tabletop exercises to assist businesses in maintaining operations and ensuring resilience during a disruption.

CHAPTER ENDNOTES

7. U.S. Department of Homeland Security, DHS Risk Lexicon: 2010 Edition (DHS, September 2010), <https://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf>.
8. U.S. Department of Homeland Security, "Designation of the National Infrastructure Protection Plan Critical Manufacturing Sector," Federal Register (April 30, 2008), <https://www.federalregister.gov/articles/2008/04/30/E8-9412/designation-of-the-national-infrastructure-protection-plan-critical-manufacturing-sector>.
9. National Association of Manufacturing, "Facts About Manufacturing," accessed September 14, 2015, <http://www.nam.org/Newsroom/Facts-About-Manufacturing/>.

4 MISSION, GOALS, AND PRIORITIES

An effective Critical Manufacturing Sector partnership is instrumental in achieving the shared security and resilience mission of the Critical Manufacturing Sector Coordinating Council and Government Coordinating Council. The councils collectively developed joint goals for sector security and resilience and corresponding priorities that the sector will pursue over the next four years. These goals and priorities directly support the NIPP 2013 goals and Joint National Priorities, as illustrated in [Appendix A](#).

CRITICAL MANUFACTURING SECTOR MISSION

Strengthen the security and resilience of the Critical Manufacturing Sector by building an active public-private partnership to coordinate efforts that enable proactive risk reduction and effective response, recovery, and adaptation.

Table 1. 2015 Critical Manufacturing Sector Goals and Priorities

Goals	Priorities
<p>1 Improve information-sharing processes and promote continuous learning through exercises, incidents, and planning to strengthen sector and cross-sector partnerships.</p>	<p>PRIORITY A Evaluate supply chain resilience and interdependencies with other critical infrastructure sectors and collaborate across sectors on risk management.</p>
	<p>PRIORITY B Increase active engagement with Critical Manufacturing Sector partners to strengthen collaboration and information sharing across member companies.</p>
	<p>PRIORITY C Work with public-private and cross-sector partners to share timely, relevant, and actionable information.</p>
<p>2 Identify and assess sector-specific threats, vulnerabilities, and consequences of inaction to raise sector risk awareness and inform risk management.</p>	<p>PRIORITY D Work with sector partners to characterize the Critical Manufacturing Sector profile of cyber and physical risks and raise risk awareness, particularly at executive levels.</p>
<p>3 Develop strategies to reduce risks to Critical Manufacturing Sector assets from human, physical, and cyber threats without hindering economic viability.</p>	<p>PRIORITY E Improve Critical Manufacturing Sector cybersecurity knowledge, tools, capabilities, and practices to secure critical cyber assets.</p>
<p>4 Support research and development, advance planning and risk mitigation, coordinated response, and rapid recovery to ensure resilient operation of critical services.</p>	<p>PRIORITY F Participate in cross-sector training and exercises to improve response and recovery capabilities to cascading disruptions.</p>

4.1 Critical Manufacturing Sector Activities

Critical Manufacturing Sector partners collaboratively developed a set of 14 activities to implement this Sector-Specific Plan and meaningfully contribute to the sector goals and priorities. The following list includes voluntary partnership activities that the sector may pursue over the next one to four years, and are not listed in any order of importance. Although Sector-Specific Plans are updated every four years, the Critical Manufacturing Sector partnership may update its activities more frequently to reflect evolving risks, changing resource allocations, and partnership progress.

Sector partners are operating in resource-limited environments. As a result, moving forward on any of the identified activities will depend largely on future resource availability, budget allocations, and sector-wide prioritization processes. Rather than develop priorities and activities based only on currently available resources, the sector identified the top activities it believes will make a significant contribution to national security and resilience. The Government Coordinating Council and Sector Coordinating Council will meet annually to prioritize and build on Sector-Specific Plan activities. During this time, the councils will further develop a list of discrete, detailed tasks to pursue over the coming year, considering timing, available resources, and feasibility.

Table 2. 2015 Critical Manufacturing Sector Activities

Map to Priority	Sector Activities
(A) (F)	1 Increase engagement opportunities between interdependent sectors; this can include full-day workshops and invitations to Critical Manufacturing Sector conferences to improve mutual understanding across sectors, share best practices, and identify shared risks.
(A) (C)	2 Identify or develop additional platforms for engagement with interdependent sectors.
(A) (B)	3 Identify supply chain resilience and risk management best practices and improve outreach.
(B) (F)	4 Work with partners to identify relevant topics for workshops, trainings, tools, and materials.
(B) (F)	5 Increase outreach, tools, and trainings targeted at small- to mid-size companies and suppliers to improve their risk awareness.
(B) (F)	6 Build on the success of the Global Crisis Response System to develop a formal structure to share private sector resources during a domestic incident.
(C)	7 Identify the most effective platform to share timely, relevant information.
(C) (F)	8 Work with partners to identify information and analytical needs, including information on how to deal with cross-jurisdictional issues, and work with international partners to address those issues and needs.
(A) (D)	9 Document risk management processes and build a compendium of best practices.
(A) (D)	10 Identify the top risks to the Critical Manufacturing Sector and across sectors to help prioritize efforts and resources.
(D) (E)	11 Define sector-specific cybersecurity risks, potential effects, and desired states for the Critical Manufacturing Sector.
(A) (D) (E)	12 Identify cybersecurity best practices for the Critical Manufacturing Sector and work with other sectors to leverage cybersecurity expertise.
(A) (D) (E)	13 Identify and benchmark risk management capabilities within the Critical Manufacturing Sector.
(B) (F)	14 Build relationships with local and regional entities through tabletop exercises, drills, and other exercises.

5 MEASURING EFFECTIVENESS

Owners and operators use a variety of indicators to measure the effectiveness and continuous improvement of their security and resilience risk management processes at the facility level. Measuring improvements in security and resilience at the sector level is far more difficult. Where possible, Critical Manufacturing Sector partners attempt to measure how their voluntary partnership activities contribute to risk reduction and enhanced resilience across the sector.

As the Sector-Specific Agency, the U.S. Department of Homeland Security has the primary responsibility for measuring and reporting progress toward sector activities using relevant metrics. An established performance metrics system designed to track the progress of sector activities is used to ensure accurate and consistent measurement.

Table 3 aligns Critical Manufacturing Sector activities with a set of possible performance metrics that the Sector-Specific Agency may use to measure and report progress, where possible. The metrics not only measure the completion of an activity—using output measures such as the number of products developed or partners engaged—but also aim to measure the outcomes of these activities—particularly how effective they are in achieving progress toward sector goals.

Within the voluntary sector partnership, often the best available outcome measure is to track intent to act based on the information, tools, or guidance received through sector activities. The Sector-Specific Agency measures this intent to act using a survey—during or following each engagement or activity—that asks three questions:

- Was the information received current and relevant?
- Will the information inform decision-making?
- Will participants share the information within their organization?

Survey results indicate the effectiveness of each activity in equipping participants with the information, tools, guidance, and processes to take actions that ultimately reduce or better manage sector risk.

The Sector-Specific Agency will report sector progress through the National Annual Report and the quadrennial Sector-Specific Plan updates. The following list is not exhaustive of all possible ways to measure effectiveness, and sector asset owners may voluntarily measure and report additional information on sector progress during the National Annual Reporting process.

Table 3. Activities and Expected Metrics

Critical Manufacturing Sector Activities	Expected Metrics
<p>1 Increase engagement opportunities between interdependent sectors; this can include full-day workshops and invitations to Critical Manufacturing Sector conferences to improve mutual understanding across sectors, share best practices, and identify shared risks.</p>	<ul style="list-style-type: none"> • Number of cross-sector conferences, workshops, and other engagements organized and coordinated by the sector • Level of participation and change in participation over time • Relevancy and intended use of the information partners receive
<p>2 Identify or develop additional platforms for engagement with interdependent sectors.</p>	<ul style="list-style-type: none"> • Stakeholder use of current information-sharing platforms, such as the Homeland Security Information Network – Critical Infrastructure, and information products • Status of developing or identifying additional cross-sector platforms, if needed • Stakeholder use of any additional platforms developed • Relevancy and intended use of the information partners receive

Critical Manufacturing Sector Activities	Expected Metrics
3 Identify supply chain resilience and risk management best practices and improve outreach.	<ul style="list-style-type: none"> • Products developed and their level of distribution (including how products are distributed and approximate number of stakeholders reached) • Number of workshops, Webinars, or other engagements designed to address supply chain resilience and the level of participation • Relevancy and intended use of the information partners receive
4 Work with partners to identify relevant topics for workshops, trainings, tools, and materials.	<ul style="list-style-type: none"> • Number of workshops and trainings held and the level of participation over time • Tools and materials developed and the level of distribution (including how tools and materials are distributed and approximate number of stakeholders reached) • Relevancy and intended use of the information partners receive
5 Increase outreach, tools, and trainings targeted at small- to mid-size companies and suppliers to improve their risk awareness.	<ul style="list-style-type: none"> • Tools, products, and trainings developed targeting this audience • Level of participation over time and/or level of distribution of relevant materials • Relevancy and intended use of the information partners receive
6 Build on the success of the Global Crisis Response System to develop a formal structure to share private sector resources during a domestic incident.	<ul style="list-style-type: none"> • Status of developing a formal structure • Level of participation in the development • Level of participation in using the structure during an incident (where possible to measure)
7 Identify the most effective platform to share timely, relevant information.	<ul style="list-style-type: none"> • Number of classified and/or unclassified briefings and forums and the level of participation • Number of meetings and workshops organized or coordinated by the sector to share information • Information products developed and the level of distribution • Relevancy and intended use of the information partners receive
8 Work with partners to identify information and analytical needs, including information on how to deal with cross-jurisdictional issues, and work with international partners to address those issues and needs.	<ul style="list-style-type: none"> • Number of engagements or workshops organized or coordinated by the sector on this issue • Products developed and the level of distribution • Relevancy and intended use of the information partners receive
9 Document risk management processes and build a compendium of best practices.	<ul style="list-style-type: none"> • Products developed and the level of distribution • Number of workshops or trainings that build awareness of best practices and the level of participation • Relevancy and intended use of the information partners receive

Critical Manufacturing Sector Activities	Expected Metrics
10 Identify the top risks to the Critical Manufacturing Sector and across sectors to help prioritize efforts and resources.	<ul style="list-style-type: none"> • Meetings and workshops organized or coordinated by the sector to identify risks • Products developed on sector risk information and the level of distribution • Relevancy and intended use of the information partners receive
11 Define sector-specific cybersecurity risks, potential effects, and desired states for the Critical Manufacturing Sector.	<ul style="list-style-type: none"> • Products developed as part of the process and the level of distribution • Relevancy and intended use of the information partners receive
12 Identify cybersecurity best practices for the Critical Manufacturing Sector and work with other sectors to leverage cybersecurity expertise.	<ul style="list-style-type: none"> • Products developed and the level of distribution • Number of meetings, workshops, and engagements organized or coordinated to discuss best practices • Relevancy and intended use of the information partners receive
13 Identify and benchmark risk management capabilities within the Critical Manufacturing Sector.	<ul style="list-style-type: none"> • Products and tools developed and the level of distribution • Level of participation in efforts to identify risk management capabilities • Relevancy and intended use of the information partners receive
14 Build relationships with local and regional entities through tabletop exercises, drills, and other exercises.	<ul style="list-style-type: none"> • Number of tabletop exercises, drills, and other exercises organized or coordinated by the sector • Level of participation over time • Relevancy and intended use of the information partners receive

APPENDIX A

Alignment with the NIPP 2013

This appendix illustrates the alignment of Critical Manufacturing Sector priorities with the NIPP 2013 national goals and Joint National Priorities and the ways in which sector activities contribute to the NIPP 2013 Calls to Action.

Table A-1. Critical Manufacturing Sector Priorities Aligned with Joint National Priorities and NIPP Goals

Critical Manufacturing Sector Priorities	Joint National Priorities					NIPP Goals
	Strengthen Management of Cyber and Physical Risks to Critical Infrastructure	Build Capabilities and Coordination for Enhanced Incident Response and Recovery	Strengthen Collaboration Across Sectors, Jurisdictions, and Disciplines	Enhance Effectiveness in Resilience Decision-making	Share Information to Improve Prevention, Protection, Mitigation, Response, and Recovery Activities	
A Evaluate supply chain resilience and interdependencies with other critical infrastructure sectors and collaborate across sectors on risk management.						
B Increase active engagement with Critical Manufacturing Sector partners to strengthen collaboration and information sharing across member companies.						Share information across the critical infrastructure community to build awareness and enable risk-informed decision-making.
C Work with public-private and cross-sector partners to share timely, relevant, and actionable information.						
D Work with sector partners to characterize the Critical Manufacturing Sector profile of cyber and physical risks and raise risk awareness, particularly at executive levels.						Assess and analyze risks to critical infrastructure (including threats, vulnerabilities, and consequences) to inform risk management activities.
E Improve Critical Manufacturing Sector cybersecurity knowledge, tools, capabilities, and practices to secure critical cyber assets.						Secure critical infrastructure against physical, cyber, and human threats through sustainable risk reduction efforts, while considering costs and benefits.
F Participate in cross-sector training and exercises to improve response and recovery capabilities to cascading disruptions.						Promote learning and adaptation during and after incidents and exercises. Enhance critical infrastructure resilience by minimizing consequences and employing effective response and recovery.

Table A-2. Contribution of the Critical Manufacturing Sector Activities to the NIPP 2013 Calls to Action

Critical Manufacturing Sector Contribution or Aligned Activity	NIPP 2013 Calls to Action											
	#1	#2	#3	#4	#5	#6	#7	#8	#9	#10	#11	#12
1 Increase engagement opportunities between interdependent sectors.						X						
2 Identify or develop additional platforms for engagement with interdependent sectors.					X	X						
3 Identify supply chain resilience and risk management best practices and improve outreach.					X	X						
4 Work with partners to identify relevant topics for workshops, trainings, tools, and materials.			X						X			
5 Increase outreach, tools, and trainings targeted at small- to mid-size companies and suppliers to improve their risk awareness.			X						X			
6 Build on the success of the Global Crisis Response System to develop a formal structure to share private sector resources during a domestic incident.							X	X				
7 Identify the most effective platform to share timely, relevant information.					X		X					
8 Work with partners to identify information and analytical needs, including information on how to deal with cross-jurisdictional issues, and work with international partners to address those issues and needs.			X		X			X				X
9 Document risk management processes and build a compendium of best practices.								X	X			X
10 Identify the top risks to the Critical Manufacturing Sector and across sectors to help prioritize efforts and resources.				X	X							
11 Define sector-specific cybersecurity risks, potential effects, and desired states for the Critical Manufacturing Sector.					X	X						
12 Identify cybersecurity best practices for the Critical Manufacturing Sector and work with other sectors to leverage cybersecurity expertise.					X	X						
13 Identify and benchmark risk management capabilities within the Critical Manufacturing Sector.					X	X						
14 Build relationships with local and regional entities through tabletop exercises, drills, and other exercises.			X					X				X
Critical Manufacturing Sector goals and priorities were developed in alignment with the 2014 Joint National Priorities in support of Call to Action #1.	X											
Development of the 2015 Critical Manufacturing Sector-Specific Plan meets this Call to Action.		X										
The Critical Manufacturing Sector supports Call to Action #10 by working with its Federal partners to implement the <i>National Critical Infrastructure Security and Resilience Research and Development Plan</i> .										X		
The measurement approach outlined in Chapter 5: Measuring Effectiveness will enable the Critical Manufacturing Sector to evaluate and report on the progress of partnership efforts in support of Call to Action #11.											X	

NIPP 2013 Calls to Action

Call to Action #1: Set National Focus through Jointly Developed Priorities

Call to Action #2: Determine Collective Actions through Joint Planning Efforts

Call to Action #3: Empower Local and Regional Partnerships to Build Capacity Nationally

Call to Action #4: Leverage Incentives to Advance Security and Resilience

Call to Action #5: Enable Risk-Informed Decision-making through Enhanced Situational Awareness

Call to Action #6: Analyze Infrastructure Dependencies, Interdependencies, and Associated Cascading Effects

Call to Action #7: Identify, Assess, and Respond to Unanticipated Infrastructure Cascading Effects During and Following Incidents

Call to Action #8: Promote Infrastructure, Community, and Regional Recovery Following Incidents

Call to Action #9: Strengthen Coordinated Development and Delivery of Technical Assistance, Training, and Education

Call to Action #10: Improve Critical Infrastructure Security and Resilience by Advancing Research and Development Solutions

Call to Action #11: Evaluate Progress toward the Achievement of Goals

Call to Action #12: Learn and Adapt During and After Exercises and Incidents

APPENDIX B

Geographic Concentration of Critical Manufacturing Facilities by Component

The transit of raw materials and finished products is a key component of the Critical Manufacturing Sector's operations. Many Critical Manufacturing Sector facilities are located along coastlines and concentrated around major freight transportation hubs, making them well-positioned for the import and export of materials and products. These maps were developed using data from the U.S. Census Bureau's "[Economic Census: Industry Snapshots, 2012](#)."

Figure B-1. Concentration of All Critical Manufacturing Facilities in 2012

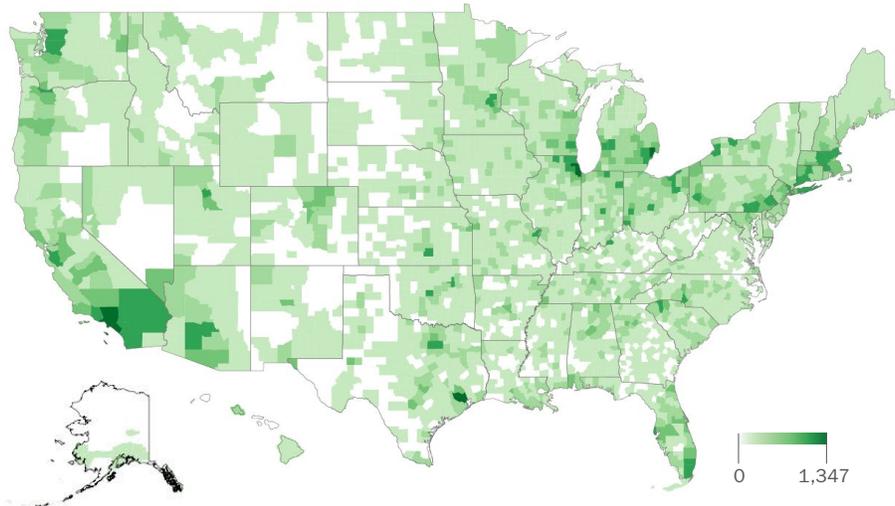
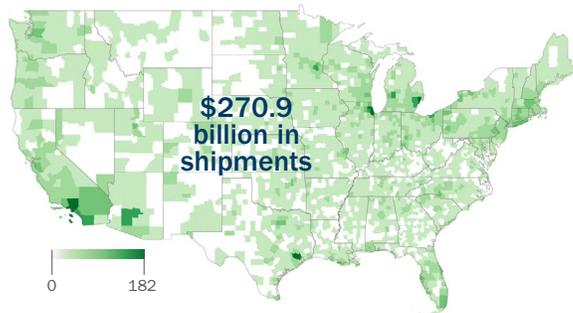
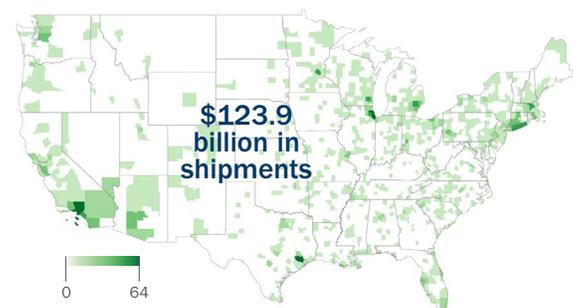


Figure B-2. Primary Metals Manufacturing



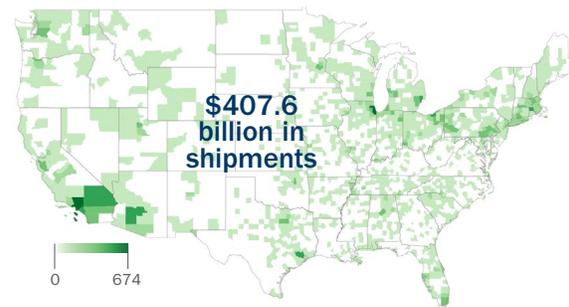
Primary Metals Manufacturing includes converting materials to assemblies, intermediate products, and end products, including iron and steel mills, ferro-alloy manufacturing, alumina and aluminum production, and non-ferrous metal production and processing.

Figure B-4. Electrical Equipment Manufacturing



Electrical Equipment Manufacturing includes specialized equipment, assemblies, intermediate products, and end products for power generation, such as transformers, electric motors and generators, and industrial controls.

Figure B-3. Machinery Manufacturing



Machinery Manufacturing includes engine, turbine, and power-transmission equipment manufacturing along with heavy-equipment manufacturing such as that used in earth moving, mining, agriculture, and construction, as well as other heavy-material handling.

Figure B-5. Transportation Manufacturing



Transportation Manufacturing includes a variety of different industries, including vehicle manufacturing, aviation and aerospace products and parts, and railroad rolling stock manufacturing.



Homeland
Security