INTRODUCTION TO THE CRITICAL MANUFACTURING SECTOR RISK MANAGEMENT AGENCY

The Critical Manufacturing Sector comprises manufacturing that is crucial to the economic prosperity and continuity of the United States. 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. Products made by these manufacturing industries are essential to many other critical infrastructure sectors, and a failure or disruption in the Critical Manufacturing Sector could result in cascading disruptions to other critical infrastructure sectors in multiple regions. The Cybersecurity and Infrastructure Security Agency (CISA), which serves as the Critical Manufacturing Sector Risk Management Agency (SRMA), and sector partners collaboratively develop guidance, resources, and training that support the security and resilience of our nation's prominent manufacturers.

CRITICAL MANUFACTURING SECTOR COLLABORATION, RESOURCES, AND TRAINING

CISA offers many resources to help owners and operators manage risks, improve security, and aid the implementation and execution of protective and response measures across the Critical Manufacturing Sector. This fact sheet lists a sampling of sector collaboration mechanisms, resources, and training materials. Unless otherwise noted, additional information can be found on the CISA website at cisa.gov/critical-manufacturing-sector.

Collaboration

Critical Manufacturing Government Coordinating Council (GCC), Sector Coordinating Council (SCC), and Working Groups convene regularly, share information, and develop tools, guidelines, and products. These groups work closely to plan, implement, and execute sector-wide resilience and security programs within the Critical Manufacturing Sector.

Critical Manufacturing Road Show annually showcases federal agency activities, promotes information sharing, and supports partnership development among Critical Manufacturing Sector stakeholders.

Regional Security Roundtables collaborate with private sector owners and operators as well as state, local, and other government partners to facilitate discussion, information sharing, and networking among stakeholders.

Critical Manufacturing Security Conference provides an opportunity annually to collaborate with sector owners and operators on security and resilience programs for physical and cyber threats.

Resources

Critical Manufacturing Sector Cybersecurity Framework Implementation Guidance provides a common language that Critical Manufacturing Sector organizations can use to assess and manage their cybersecurity risks and uses the National Institute of Standards and Technology (NIST) voluntary Framework for Improving Critical Infrastructure Cybersecurity.

Department of Homeland Security (DHS)-Sponsored Private Sector Security Clearance Program allows critical infrastructure owners and operators to apply for a secret-level security clearance and share classified information relevant to the security and resilience of the Nation's critical infrastructure.

The Critical Manufacturing Security Guide consolidates effective industry security practices into a framework for owners and operators to implement security activities and measures that promote the protection of personnel, public health, and public safety.

Training

Business Continuity Planning Suite helps businesses create, improve, or update their business continuity plans with scalable, easy-to-use software. Learn more at ready.gov/business-continuity-planning-suite.

Active Shooter Preparedness Materials include a workshop series, online training, educational videos, and "How to Respond" resource materials, such as reference posters, guides, and cards. Learn more at cisa.gov/active-shooter-preparedness.

Online Training Courses on active shooter preparedness, insider threat, surveillance detection, and more are self-paced and available at no-cost.

Counter-Improvised Explosive Device Training and Awareness course options include bombing prevention workshops, soft target awareness, and surveillance detection.

SECTOR PROFILE

Critical Manfucturing Sector assets are privately owned and operated and include manufacturing facilities, processing and distribution facilities, sales offices, corporate headquarters, and product storage. 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. Central to the sector's operations is the global transport of raw materials and finished products along large supply chains. 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.

Sector Components

Primary Metals

Processes aluminum, iron, and steel that support transportation, urban centers, energy supply, clean water, safe food, and defense.

Machinery

Manufactures engines, turbines, power-transmission equipment, and heavy machinery.

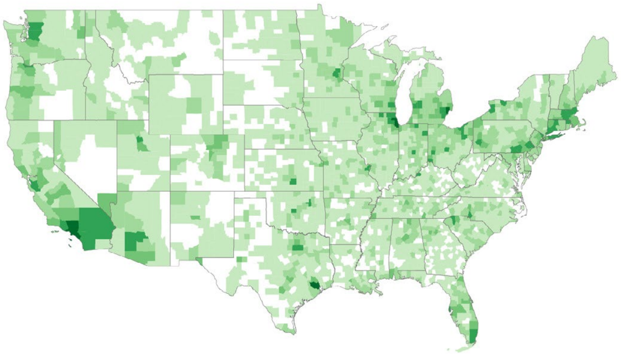
Electrical Equipment, Appliance, & Component

Manufactures specialized power generation equipment, including critical transformers and generators.

Transportation

Manufactures critical components for cars, trucks, commercial ships, commercial aircraft, and rail parts for both passenger and freight.

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, https://www.census.gov/programs-surveys/economic-census.html.

CRITICAL MANUFACTURING SECURITY PRIORITIES

- **Active Shooter Prevention:** The economic, strategic, and iconic value of the sector may make it an attractive target for criminals who aim to destroy facilities or interfere with manufacturing operations.
- **Counterfeit Prevention:** Counterfeit parts or components entering the supply chain are a significant threat to critical manufacturing operations. Counterfeit components can significantly reduce the quality and safety of manufacturing products, potentially leading to accidents, lawsuits, or the loss of market share or competitiveness.
- **Cybersecurity:** 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 and affect business reputation.
- **Disaster Area Access:** Implementation of electronic access controls may help to detect and assess a security incident during a disaster. Access to assets and facilities should be limited to authorized users, processes, or devices.
- **Information Sharing:** Information sharing is key in implementing a successful cybersecurity framework. Information should be shared among management and operations personnel operating within the physical and cyber space.
- **UAS Protection:** All uncrewed aircraft systems (UAS) utilized by owners and operators that weigh more than 0.55 must be registered. Additionally, ensure that the data captured by your UAS is protected. See the CISA website for more detailed information on how to secure your UAS.