CRITICAL MANUFACTURING SECTOR

Security Guide

JULY 2020

Cybersecurity and Infrastructure Security Agency

Contents

Executive Summary

The Critical Manufacturing Sector comprises processes and products that are crucial to the economic prosperity and continuity of the United States. Among myriad roles and responsibilities, 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. The Critical Manufacturing Sector 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, complex supply chains.

Risks to physical and cyber assets in the sector originate from multiple sources, including deliberate, malicious human actions (e.g., crime, sabotage, and terrorism); non-malicious human actions (e.g., accidents and negligence); technological deficiencies; and natural disasters. A failure or disruption of operations in the Critical Manufacturing Sector could result in cascading disruptions to other sectors in multiple regions. Each owner or operator manages unique assets; a distinct risk profile; and tailored operational processes, business environments, and security practices.

The overall security level of individual assets evolves over time and varies in accordance with site-specific conditions and threats. Owners and operators can identify critical assets on which to focus additional security reviews, determine the level of risk that is practical and acceptable for their assets at a particular point in time, and implement security practices appropriate to the level of risk and resources available. The wide range of sector security practices includes research and development efforts, multi-jurisdictional regional exercises, comprehensive training and outreach initiatives, and implementation of plans to support incident preparedness, response, and restoration. These practices are often guided or directed by requirements associated with industry standards. Despite variances in regulatory control, specific security practices can aid any Critical Manufacturing Sector owner or operator with identifying, understanding, and mitigating risk to assets, systems, and networks.

The *Critical Manufacturing Security Guide* consolidates effective industry security practices into a framework for owners and operators to select and implement security activities and measures that promote the protection of personnel, public health, public safety, and public confidence. Owners and operators may review the document in full or focus their review on specific security practice components that address their security needs or augment existing security practices. For additional information about the Critical Manufacturing Sector composition, risk profile, and risk management activities, refer to the *Critical Manufacturing Sector-Specific Plan* located at www.dhs.gov/critical-manufacturing-sector.

> *Critical infrastructure owners and operators are uniquely positioned to manage risks to their individual operations and assets, and to determine effective strategies to make them more secure and resilient.*
>
> – **Presidential Policy Directive 21**

Security Practices

On a daily basis, owners and operators take actions that support risk management planning and investments in security as necessary components of prudent business planning and operations. The security practices of each owner and operator—which range from implementing select risk management activities and measures to enacting and monitoring a formal security program—help increase organizational safety and security, safeguard personnel, and prevent unauthorized access to assets, business processes, control systems, equipment, and sensitive information. By applying basic security fundamentals and industry effective practices, owners and operators can identify and implement security measures consistent with the

criticality of the site and business processes and appropriate for the level of acceptable risk for each facility selected for enhanced security.

Critical Manufacturing Sector security programs will vary, as they are tailored to the specific facility characteristics, needs, and risk profiles. However, owners and operators engaged in starting or enhancing security programs for their facilities should consider common security program administrative and strategic fundamentals. These administrative basics include the following:

- **Comprehensive risk analysis**, including risk assessments, drives effective security programs. Understanding the risks to critical assets dictates how to address those risks and supports justification for security measures. Risk analysis leads to the critical buy-in needed from executives and other stakeholders in the organization to carry out security improvements.
- **Personnel and resources dedicated specifically for security** support the effectiveness of security programs by maintaining focus and accountability and minimizing the pressure of other priorities that may hinder the implementation of effective security practices.
- **Partnerships with federal, state, and local officials** enhance security programs. Local law enforcement, fire department personnel, and other first responders are key partners in preparedness and response and in understanding facility details and risks. State and local government officials are valuable partners for security training and exercises. Federal partners offer information, intelligence sharing, and programs for assessment, training, and regulatory compliance.

Valuable tools, training, and programs that may help Critical Manufacturing Sector stakeholders implement fundamental security practices are described in Appendix B, including the U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) Protective Security Advisor Program (PSA), the DHS Homeland Security Information Network (HSIN), and the Federal Bureau of Investigation (FBI) InfraGard partnership.

CISA Protective Security Advisor Program

HSIN | Homeland Security Information Network

InfraGard Partnership For Protection

- **Information-sharing organizations and platforms** are highly valuable for ensuring security programs are up to date with risk, threat, and intelligence information relevant to the security of facilities.

For many owners and operators, the level of security investments reflects risk-versus-consequence tradeoffs that are based on two factors: what is known about the risk environment and what is economically justifiable and sustainable in a competitive marketplace or within resource constraints. Further, security enhancement investments often compete with other investments, with many decision makers finding it difficult to justify security expenditures without a strong business case. By systematically leveraging industry effective practices such as those identified in the *Critical Manufacturing Security Guide* (and tied to business objectives), owners and operators can target security investments for specific assets based on assessed risk and associated security measures to reduce risk. Benefits may include satisfying safety and security requirements, improving brand image and competitiveness, increasing preparedness, reducing impacts and frequency of disruptions, and realizing cost efficiencies through streamlining and integrating security processes.

Identifying critical assets represents the first step in systematically increasing security by applying targeted security measures. Owners and operators can identify and prioritize critical assets based on industry standards, company policies, or regulatory guidelines. After identifying and prioritizing assets, owners and

operators can implement security practices, including assessments and security measures. Though Critical Manufacturing Sector security practices are frequently integrated across the enterprise (especially with increasingly converging physical and cyber technologies), they can be organized into four major categories: physical, cyber, personnel, and supply chain. The following briefly summarizes these practices, with additional information on the various tools, capabilities, and references available to owners and operators found in the respective document chapters.

Physical Security Practices: Security risk assessments that feature threat, vulnerability, and consequence components can help owners and operators make cost-effective risk mitigation investments across their portfolios. An owner or operator may choose to conduct an individual assessment to understand a specific component or implement a full, comprehensive security risk assessment to incorporate all three individual components. A variety of physical security measures could then be selected to mitigate risk. Such measures are generally designed and installed to perform the specific functions in relation to an attack or disruption of an asset (e.g., prevent or deter, detect and assess, respond, and restore). An owner or operator may choose to implement particular physical security measures to improve those functions or implement a comprehensive approach that integrates multiple functions.

Cybersecurity Practices: Security in the Critical Manufacturing Sector is not limited to the physical environment but encompasses the ever-evolving cyber environment. Enhancing security and resilience in the cyber realm begins with identifying and assessing critical cyber assets and systems, as well as the facility's and connecting networks' cyber risks and vulnerabilities. Deficient cybersecurity functions can then be selected for further analysis. Once the cyber landscape has been understood, the owner or operator is able to implement targeted cybersecurity practices to improve the cybersecurity posture and address the risks and vulnerabilities uncovered. In implementing cybersecurity practices, owners and operators may choose to implement practices to address select deficiencies. However, given the evolving cyber landscape and myriad unknowns, owners and operators may best improve their cybersecurity posture through persistent implementation of comprehensive cybersecurity risk management: identify, protect, detect, respond, and recover.

Personnel Security Practices: Owners, operators, personnel, and contractors all perform mission-critical tasks to operate assets, systems, and networks and implement security measures. The errant or illicit actions of one person can cause catastrophic damage to manufacturing assets and processes, or harm sector personnel or the public. Assessing threats includes conducting background screening for potential and new hires or contractors, periodically rescreening existing personnel, and determining the likelihood of, and vulnerability to, insider threats. Personnel security measures include background investigations, training to increase security awareness and education, exercises and drills to hone skills and knowledge related to specific types of security incidents, and development and management of response and recovery plans.

Supply Chain Security Practices: Supply chain disruptions are of significant concern to Critical Manufacturing Sector owners and operators. With stringent manufacturing schedules, just-in-time orders, and narrow profit margins around a complex amalgamation of multi-tier suppliers, vendors, and customers, disruptions in Critical Manufacturing Sector supply chains can inflict cascading effects across multiple sectors, industries, and economies. To address threats to and vulnerabilities of supply chains in the sector, owners and operators apply effective risk management practices such as industry supply chain risk assessment standards, innovative planning policies for incident prevention, and adaptive mechanisms to quickly detect and address disruptions as they occur. Such foundational supply chain risk management practices drive the need to meet performance standards and customer demands, manage brand reputation and integrity, and justify the economic return for investments.

How to Use the *Critical Manufacturing Sector Security Guide*

The *Critical Manufacturing Sector Security Guide* consolidates effective industry security practices into a framework to help owners and operators select and implement security activities and measures that reduce

risk; improve the protection of personnel, public health, and public safety; and reinforce public confidence. Specifically, the *Critical Manufacturing Sector Security Guide* outlines various strategies and methods to help select and implement security activities and measures appropriate to a facility. Each section of the document focuses on a distinct aspect of sector security practices—physical, cyber, personnel, and supply chain—and includes industry-recognized effective practices and means by which to obtain additional information. Links to documents referenced herein are located in Appendix A: Resources.

Owners and operators are encouraged to review the information contained in the *Critical Manufacturing Sector Security Guide* and implement the security practices appropriate for the facility's risk profile, operational processes, business environments, and available resources. It is important to note that, though this document separates the security topics into different chapters, many of the practices are inextricably linked. For example, many critical physical assets are controlled, operated, and maintained through cyber infrastructure. Further, all physical, cyber, personnel, and supply chain security measures rely on adequate information security measures to be effective. As such, users of the *Critical Manufacturing Sector Security Guide* need not proceed sequentially through the chapters and may instead select the sections of most interest.

Disclaimer

The information provided in the *Critical Manufacturing Sector Security Guide* is not intended to supersede, modify, or replace any existing codes, standards, or policies applicable to the sector. The publication of the *Critical Manufacturing Sector Security Guide* does not constitute endorsement of any product or product type, nor does it test, certify, or approve any products. The use of this document is entirely voluntary. Some resources and tools identified in this document may require a paid subscription and/or organizational membership. The use of any purchased resource or tool is at the discretion of the organization. The *Critical Manufacturing Sector Security Guide* recognizes that the overall level of security will vary in accordance with site-specific conditions and specific threats to each individual asset. Each owner and operator must decide the level of risk that it is considered practical and acceptable, as well as the corresponding security practices.

Physical Security Practices

The cornerstone of maintaining Critical Manufacturing Sector facility security and resilience is the collective array of physical security practices that protect and secure critical assets. Identifying critical assets provides the starting point for an integrated approach to physical protection, with owners and operators utilizing a variety of methods to identify and prioritize assets. Owners and operators can identify critical physical assets based on criteria relating the value of an asset to the organization's strategic and operational objectives. Though these objectives vary from site to site, common references for identifying critical physical assets in the Critical Manufacturing Sector include:

- American National Standards Institute (ANSI) Risk Assessment Standard (RA.1-2015)
- Carnegie Mellon University, Software Engineering Institute, Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)
- The Open Group Factor Analysis of Information Risk (FAIR)

These methods also are key resources for the risk assessments in the subsequent section of this chapter. Appendix C provides considerations for evaluating business assets and functions for criticality.

Following the identification of critical assets, subsequent security risk assessments that feature threat, vulnerability, and consequence components can help owners and operators make cost-effective risk mitigation investments across their portfolio. An important consideration for owners and operators is to ensure that business leadership, rather than security divisions, has ownership of critical asset identification and assessment to drive organization buy-in for physical (and cyber) security practices.

Owners and operators may then choose to implement physical security measures for mitigating risk in different ways, according to the defining characteristics and operating environments (including industry codes and standards) of their portfolios. Options range from adopting or expanding distinct security measures (e.g., surveillance, access control, and barrier systems) to developing and administering a comprehensive physical security plan. Owners and operators can choose to conduct the level of risk assessment that is most appropriate to their objectives. This may entail conducting a full, comprehensive risk assessment or an individual consequence, vulnerability, or threat assessment for a specific purpose.

Critical Manufacturing Sector facilities and organizations confront numerous risks to physical security. Major physical security issues of concern for the Critical Manufacturing Sector include natural disasters and extreme weather and deliberate attacks on sector assets.

- **Natural Disasters and Extreme Weather:** The natural disasters of greatest concern to the Critical Manufacturing Sector in selected regions include earthquakes in the Western and Central United States, flooding along the Gulf Coast and in the Central United States, hurricanes along the Atlantic and Gulf Coasts, and tornadoes in the Midwest and South. Disruptions in surface, rail, barge, and pipeline transportation associated with natural disasters and extreme weather are also of great concern.
- **Deliberate Attacks:** The economic, strategic, and iconic value of the sector may make it an attractive target for those who aim to destroy facilities or interfere with manufacturing operations. Physical attacks that can threaten Critical Manufacturing Sector assets include sabotage of equipment, parts, or processes; vehicle attacks to damage facility operations, breach security barriers, convey explosive attacks, or trigger environmental disasters; and active shooter incidents.

Owners and operators may address these or other prominent physical security issues by conducting physical security risk assessments and implementing physical security measures.

Physical Security Risk Assessments

A thorough and complete risk assessment is a common industry approach by which to define appropriate physical security practices. Risk is understood as the probability of an undesirable event occurring, or the capacity for a potential loss and its probability of occurrence. Assessing risk entails identifying the undesired event (or consequence) and the probability of its occurrence, which includes examining threat and vulnerability. While assessment methodologies may vary in scope, the foundational understanding of risk remains the same.

Figure 1. Risk is assessed as a function of consequence, vulnerability, and threat.

Physical security is assessed through a risk-based process in which risk is assessed as a function of threats, vulnerabilities, and consequences (as depicted in Figure 1). Although these risk components are standard, the wide variation of assets within the Critical Manufacturing Sector motivates sector partners to use a range of individual threat, vulnerability, or consequence assessment methodologies and/or comprehensive risk assessment methodologies.

Most security risk assessments are informed by all of the individual types of assessment—threat, vulnerability, and consequence. However, an owner or operator may choose to conduct an individual risk assessment to understand a specific security component of the facility or asset. The risk assessment conducted is only as good as the accuracy of the variables entered into the equation. Calculating absolute risk—based on specific standard units of risk measurements—may be challenging, as it is often based on limited or imperfect information. Instead, the owner or operator may find it more meaningful and manageable to calculate relative risk based on measuring risk as a ratio. In calculating relative risk, the owner or operator compares the risk value of the scenario relative to other similarly constructed risk values. In addition, utilizing relative risk avoids the disclosure of sensitive information but still conveys to decision makers the significance of the risk.

Consequence Assessment

Consequence is measured as the range of loss or damage resulting from an undesired event. The determination of the consequences of an attack on a critical asset must consider both catastrophic events that result in total failure and attacks that result in the asset operating at a reduced capacity. A full consequence assessment takes into consideration specific public health and safety, economic, psychological, and governmental impacts. The four main categories of consequence include:

- **Public Health and Safety:** Effects on human life and physical well-being (e.g., fatalities and injuries)
- **Economic:** Direct and indirect effects on the economy (e.g., costs to rebuild the asset and costs to respond to and recover from an attack)
- **Psychological:** Effects on public morale and confidence in national economic and political institutions
- **Governance/Mission Impact:** Effects on the government's ability to maintain order, deliver minimum essential public services, ensure public health and safety, and carry out national security-related missions

At a minimum, consequence assessments focus on two fundamental impacts: human (loss of life) and direct economic impacts. Both of these fundamental impacts can be referenced during the initial asset identification process to help determine whether an asset is defined as a critical asset. If multiple critical assets are present, then each asset may be evaluated separately for consequences. Once the consequence of each critical asset disruption has been established, the owner or operator can rank each asset by its criticality and create a prioritized list of critical assets. The fundamental impacts for a minimum consequence assessment include:

- **Loss of Life:** The expected number of fatalities from the event. Calculating loss of life requires an understanding of the total population at risk.
- **Economic Impact:** The total economic losses that may occur. Calculating economic impact includes the estimation of lost facility revenues, lost benefits during disruption, costs to recover operations to full operating capacity, replacement costs of damaged or destroyed assets, and environmental damage costs.

Vulnerability Assessment

Vulnerability is measured as the probability that an adversary would be successful in an attack and that the assets or components would be compromised. Determining this measurement includes assessing how easy the attack would be, how long it would take, and how likely it is that the adversary is caught. Vulnerabilities include an asset's, system's, or network's design, location, security posture, process, or operation if one of these characteristics render the component susceptible to destruction, incapacitation, or exploitation. A vulnerability assessment will identify areas of weakness that could result in undesired consequences, taking into account intrinsic structural weaknesses, protective measures, resilience, and redundancies. In trying to identify security vulnerabilities, potential aggressors may conduct sophisticated surveillance over a long period of time; this activity can be difficult to detect. The overall objective of surveillance activity is to determine possible targets, attack modes, and likelihoods of success. Potential aggressors may seek to identify such features as presence or absence of security cameras, identification cards of personnel or contractors/vendors, or security event response types and timing.

DHS offers a valuable tool to support Critical Manufacturing Sector vulnerability assessments:

- **Infrastructure Survey Tool (IST):** The IST is voluntary web-based security survey conducted by a DHS Protective Security Advisor in coordination with facility owners and operators to identify a facility's overall security and resilience. The survey contains more than 100 questions used to gather information on such things as physical security, security forces, security management, information sharing, and protective measures. The IST results inform owners and operators of potential vulnerabilities facing their assets or systems and recommend measures to mitigate those vulnerabilities. Facility owners access results and preview the effects of proposed mitigation measures through the interactive IST Dashboard.

Threat Assessment

Threats represent the probability of an attack by an adversary based on an analysis of motivation (intent) and capability. New or evolving threats to the continued reliability and integrity of infrastructure necessitate education and vigilance. The more the owner or operator knows about the actual and potential threats to the facility's operations and mission, the more effective are the measures taken by the organization to protect its assets. DHS has instituted the National Terrorism Advisory System (NTAS) to provide alerts on terrorist threats. In addition, owners should perform exercises to test and improve their security operations and plans prior to an actual threat level increase.

The threat environment for the Critical Manufacturing Sector may be highly variable, but understanding common threat types will help the owner assess threats against facilities and assets. Common physical

security threat types are associated with the major physical security issues described above: natural disasters and extreme weather and deliberate attacks on sector assets.

Threat assessments analyze, evaluate, and quantify the threat variable of the risk equation. An assessment includes examining the likely tactics, techniques, and procedures (e.g., attack methodology and types of weapons) used to carry out an attack. A threat assessment begins by identifying critical operations and assets within a facility. The assessment is a snapshot in time and may be performed periodically to ensure that the most up-to-date and available information is used during the assessment process. A threat assessment comprises three main areas:

- **Internal Threat Assessment:** Understanding one's own organization and personnel is key when protecting critical assets. The internal portion of a threat assessment commonly takes into account all of the staff, including personnel and contractors/vendors that have access to the facility and critical assets and operations. Developing an organization-wide program for deterring, detecting, and mitigating insider threats may include establishing an information-sharing process among human resources, intelligence, law enforcement, and other sources based on procedures compliant with all applicable laws and privacy requirements. A review of human resource and workforce relations actions and incident reports, provided by the human resources department or facility manager, can serve as a source for identifying personnel who may have malicious intent.
- **External Threat Assessment:** When performing the external portion of the threat assessment, it is advisable to involve local, state, and federal law enforcement agencies. Such agencies can provide historical data and information on groups or individuals living or operating in the vicinity, and can keep owners and operators abreast of important changes in the threat environment. The Internet is another source for threat information. Information provided by these sources can augment information provided through a review of the facility's logs of security incidents and investigations. Supply chain security is an important component of external threat assessments and is discussed in more detail in the Supply Chain Security Practices chapter.
- **Quantification and Application:** Once the internal and external threat information is acquired, it can be quantified and applied to the specific critical asset. By quantifying these areas, owners and operators can determine the likelihood of an attack and prioritize and plan for potential incidents, as well as implement appropriate security measures.

Comprehensive Security Risk Assessment

A security risk assessment is the comprehensive process of collecting information and assigning values to risks to make informed decisions pertaining to the management and mitigation of risk. The purpose of a security risk assessment is to identify critical assets and components, determine threats, and assess vulnerabilities and consequences continuously. A comprehensive security risk assessment will assist the decision maker with making cost-effective investments in risk mitigation options to optimize expenditures and maximize performance of security countermeasures.

When performing a security risk assessment, an assessment team familiar with the type of facility and the components that are critical for the facility's operation can effectively understand disruption consequences. Once the vulnerability of the critical

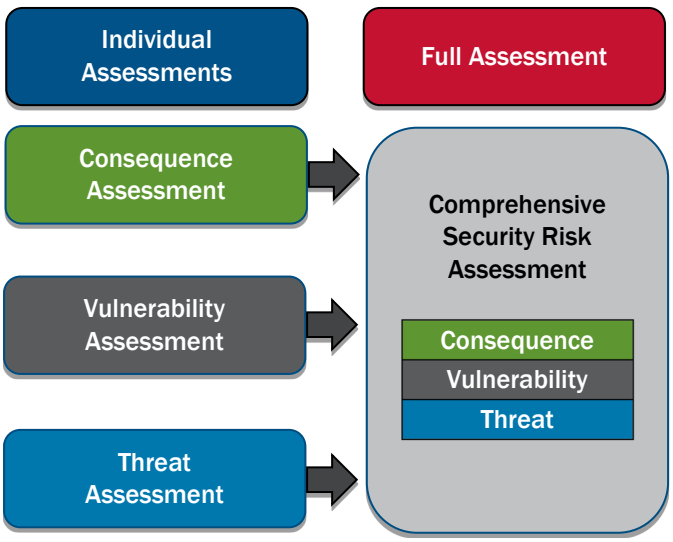

Figure 2. Individual assessment inputs into a comprehensive security risk assessment

assets and components is assessed, an evaluation of the perceived threat can be applied to estimate the overall risk and to help establish a strategy for protection, response, and/or recovery. Risk assessment is an ongoing process that should be closely monitored, conducted periodically, and reassessed and modified as needed to protect critical assets. At a minimum, updates should be performed when site or threat conditions change.

Multiple security risk assessment methods are available to owners and operators, including the individual consequence, vulnerability, and threat assessments mentioned above. In addition to the risk assessment methodologies mentioned above (ANSI RA.1-2015, OCTAVE, and FAIR), other methodologies and resources that can be used to develop customized risk assessments for individual site needs include:

- CBP CTPAT Risk Assessment
- U.S. Department of Defense (DOD) Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs
- DHS Chemical Security Assessment Tool (CSAT)
- International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) Risk management – Risk assessment techniques (ISO/IEC 31010)
- Transported Asset Protection Association (TAPA) Facility Security Requirements (FSR)

Physical Security Measures

Understanding consequences, vulnerabilities, threats, and overall risks for critical assets through assessments affords sector owners and operators the opportunity to select and implement physical security measures that may best address those risks. The basic principles of physical security are similar across many types of structures or components. The main differences for physical security among asset types are the degree of security required and the sophistication of layered protection needed to properly secure each asset.

When choosing physical security measures for critical assets, it is important to consider some fundamental concepts. Physical security measures are generally designed and installed to perform specific functions in relation to an attack or disruption of an asset: prevent or deter, detect and assess, respond, and restore. Depending on the results of assessments, industry codes and standards, and available resources, owners and operators may choose to implement particular physical security measures to improve those functions, or may adopt or expand on a comprehensive approach to implementing physical security measures. Whether specific or comprehensive, either path may include developing or adapting strategic plans for the facility or portfolio (such as a physical security plan, a business continuity plan [BCP], or an emergency action plan [EAP]) to incorporate new or updated physical security measures.

Regardless of the physical security measures implemented or strategic plans in use, collaboration across the entire organization is important to ensure that physical security practices are effective and efficient.

Prevent or Deter

The presence of visible security features and operations may deter an adversary from attacking or disrupting an asset or corresponding components. Although it is difficult to determine the level of effectiveness of deterrence measures, visible security features and operations may help owners and operators prevent common minor incidents such as vandalism and theft. Deterrence measures (e.g., visible barriers, surveillance cameras, intrusion detection sensors, protective lighting, and the presence of security officers) may help to deter an adversary and prevent an incident before it occurs. In addition to preventing unauthorized facility access, these security measures are designed to safeguard personnel.

Physical security preparedness may also include identifying and ensuring the availability of materials, equipment, and personnel needed for an emergency response. Certain types of disruptions might result in

temporary or permanent loss or incapacitation of key personnel, making the designation of decision-making authority in advance of various circumstances a critical component to preparedness. It may be necessary to identify whether any critical skills reside with just one individual such that loss of that person would seriously interfere with safe facility operations. Training and exercises can be periodically conducted to demonstrate actions to be taken during disruptions, as well as practical considerations and limitations that may otherwise be overlooked in a written security plan but that may be addressed in a BCP or EAP. Examples of security measures are described in greater detail under other general physical security functions listed below.

Business Continuity Plans

Business continuity emphasizes the value in ensuring that, in the event of a disruptive incident, operations and vital functions can continue without a severe drop in services. The process for BCP development commonly includes four steps:

- Conduct a business impact analysis to identify time-sensitive or critical business functions and processes and the resources that support them.
- Identify, document, and implement plans to recover critical business functions and processes.
- Organize a business continuity team and compile a business continuity plan to manage a business disruption.
- Conduct training for the business continuity team and testing and exercises to evaluate recovery strategies and the plan.

General guidance for owners and operators on BCPs is available through the Critical Manufacturing Sector Business Continuity Planning Suite and the Disaster Recovery Institute International (DRI International) Professional Practices for Business Continuity Management.

- **BCP Suite:** The BCP Suite, managed by DHS, enables Critical Manufacturing Sector organizations to create, improve, or update BCPs. The suite is user-friendly and scalable for optimal organizational use. It consists of three main components: BCP training, automated BCP and disaster recovery plan generators, and a self-directed exercise for testing an implemented BCP.
- **DRI International Professional Practices for Business Continuity Management:** This framework assists owners and operators with developing, implementing, and maintaining business continuity programs and plans. The framework also can serve as a means for assessing an organization's business continuity capabilities and identify gaps and opportunities for improvement.

Emergency Action Plans

EAPs are common strategic plans used by Critical Manufacturing Sector owners and operators. These plans broadly cover the safety of a facility and may be required by regulation or industry standards. Though EAPs are intended for safety incidents, their content makes them valuable for planning or response related to security incidents. Because of common requirements for EAPs, many sector owners and operators already have plans, procedures, and measures in place at their facilities. These can be incorporated into a comprehensive physical protection system. To maintain strategic plans in a single document, an owner or operator may choose to include separate annexes for physical and site security within the facility EAP.

Regardless of how these strategic plans are organized, comprehensive physical protection systems are intended to be flexible and have the ability to change as the threat levels increase or decrease. Example measures may be tailored for each individual facility. As threat conditions change, the system can be modified to effectively mitigate the associated risk (including periodic updates to threat identification portions of strategic plans). Owners and operators can develop active plans that, in advance, direct security resources and procedures for increasing levels of security protection as the threat landscape intensifies. Active plans support the ability to rapidly change the security posture for local and regional threats that may arise quickly based on specific issues in the area, such as a protest or localized increase in copper theft.

One approach to determining when to increase security measures is to follow the DHS NTAS alerts, which indicate whether the threat is elevated or imminent. If NTAS alerts indicate credible threats of terrorism related to the Critical Manufacturing Sector, owners and operators may choose to elevate their security measures. The NTAS website (www.dhs.gov/national-terrorism-advisory-system) is the authoritative source for information about the current NTAS level. An NTAS alert will be issued only when credible information is available and will be based on the nature of the threat. Additional information on EAPs is included in the Respond and Recover section of the Personnel Security Practices chapter.

Detect and Assess

Implementation of security measures such as intrusion detection systems, monitored video surveillance systems, protective lighting, and electronic access controls may help to detect and assess a security incident. Enacting quality control measures of product development may also help to detect and assess security problems in product manufacturing. Security officers may help to detect an event during patrols, but they are often better suited to assessing events than performing incident detection. Detection systems often have very high nuisance and false alarm rates; therefore, detection without proper assessment is typically not considered detection of an event. Common examples of measures used for detection and assessment of physical security incidents are listed below. As many of these detection measures are technological, owners and operators leveraging such measures may also consider hardening or otherwise securing (with physical reinforcement, barriers, or other non-technological protection) the energy supply required for operation.

- **Intrusion Detection Systems:** These systems use sensors, alarm systems, security personnel, and other methods to alert site personnel of unauthorized access to the site, area, or system. Detection equipment and the systems that coordinate that equipment can be leveraged to identify intrusions in a timely manner and accurately characterize them. Automated intrusion detection technologies are particularly beneficial in their ability to detect and catalog events more reliably than personnel alone over extended periods of time. However, personnel often excel at assessing situations and are an important component of every intrusion detection system.
- **Surveillance Systems:** These systems commonly incorporate both natural surveillance and electronic surveillance system characteristics into one effective program. Surveillance cameras are crucial to any security program, as they can provide the ability to witness and record incidents, which can help to identify suspects, protect against liability claims, and be used as an effective investigation tool. Furthermore, video analytics (i.e., the analysis of surveillance camera recordings) may be used to combine surveillance and intrusion detection systems data to enhance situational awareness and potentially detect otherwise unknown incidents or trends that may compromise physical security.
- **Protective Lighting:** Protective lighting is a critical physical security feature, as many malicious acts are committed during night hours. The mere ability to detect and assess nighttime incidents may offer a deterrent, proactively preventing such attacks. In addition, proper protective lighting may improve the effectiveness of the surveillance system, depending upon the type of surveillance technology in use at the site.
- **Security Officers:** The available security forces (including onsite personnel and local law enforcement); their coverage of assets; and their ability to respond, interrupt, and neutralize adversaries are highly valued components of physical security. Owners and operators may choose whether the officers are to be onsite, armed or unarmed, contract officers or hired personnel, or some combination thereof. The choice of onsite security officers may require a significant investment that could demand a large portion of a facility's security budget.

Respond

Effective incident response and associated communications are critical for physical security. During an incident, swift and accurate communications to and among a response force are crucial. In addition, the time it takes for an effective response force to respond, interrupt, and neutralize an adversary is the basis

for determining many requirements for physical protective measures. Therefore, understanding the response time for those responsible for protecting the facility, such as local or state law enforcement officials, is an important step in implementing response security measures. The time it takes to detect, assess, communicate, and respond to the incident can dictate the type of security measures to be used to best protect critical assets. Key measures for effective incident response include:

- **Communications:** The integration of the different security measures, technologies, and personnel is a vital part of managing and developing an effective protection program. Such integration includes day-to-day and redundant emergency communication systems and equipment for critical communication pathways. Communication methods often include wired and wireless networking to transmit security feeds from detection and surveillance systems. As a result, the convergence of physical and cybersecurity is increasingly common; a collaborative effort may be developed, enhanced, and promoted between information technology (IT) and security personnel. See the Cybersecurity Practices chapter for more information.
- **Response Forces:** Security personnel are the major component of effective incident response. A response force may include just one security or local law enforcement officer or may be expanded to include dedicated teams of personnel trained and activated for specific events, such as special weapons and tactics (SWAT) teams or public safety bomb squads. Response force requirements relative to specific facility or asset vulnerabilities may be identified in vulnerability assessments as described in the Conduct Physical Security Risk Assessments section of this chapter.
- **Safeguarding Personnel:** During an incident, controlling access—such as through a physical security boundary—is designed to restrict entrance and exit movement to authorized personnel and resources. This provides protection not only for the facility but also for personnel within the facility.

Restore

Efficient and effective restoration and recovery after an incident or disruption may mitigate the adverse effects of high-consequence events. Since it is difficult and expensive to prevent some of the greatest threats to critical assets, the ability to recover from a high-consequence event is paramount. Physical security measures in place for the restore function may often reduce the effects of an incident and, in some cases, may be the only way to effectively protect a facility or its critical assets from certain threats.

- **Resources:** Supply chain flexibility, stockpiles of replacement parts, and contractual support for recovery operations are highly valuable components that may be used to restore critical assets and functions.
- **Mutual Aid:** Mutual aid agreements with other Critical Manufacturing Sector facilities, companies, or vendors or with other critical infrastructure owners and operators (especially from the Chemical, Energy, Transportation Systems, and Water and Wastewater Systems Sectors) are commonly leveraged in planning for recovery and restoration.

Comprehensive Physical Protection System and Procedures

Many sector owners and operators employ a comprehensive physical protection system to mitigate risks to their assets. A comprehensive system merges people, procedures, and equipment into a single methodology. Owners and operators may approach system integration by developing and maintaining a physical security plan, which describes all physical security measures and procedures to best ensure security within the full range of threat conditions. Similar assets may need very different physical security measures and procedures; no two physical security plans are exactly the same. In addition, the physical security plan may be incorporated into a comprehensive site plan, as some owners and operators may choose to combine multiple strategic documents into one that includes physical security, response, and recovery plans, as well as BCPs or EAPs. These plans often have provisions for personnel safety and security, especially relating to evacuation from the site of an incident. A sample security plan outline is included in Appendix D.

Cybersecurity Practices

To enact a robust approach to cybersecurity, owners and operators identify critical cyber assets and systems, in addition to cyber risks and vulnerabilities. After identifying these cyber assets, systems, risks, and vulnerabilities, owners and operators can then implement cybersecurity practices designed to improve their cybersecurity postures, prevent or mitigate cyberattacks, and ensure the continuity of facility operations and services. An owner or operator may choose to use a cybersecurity assessment to identify specific security gaps and prioritize actions accordingly to improve cybersecurity, or may develop and administer a comprehensive cybersecurity plan inclusive of identify, protect, detect, respond, and recover functions.

Cybersecurity of the industrial control systems (ICSs) that monitor, automate, and control critical manufacturing processes is a significant focus for sector owners and operators. These control systems collect information about operations and component status to manage, command, or regulate key components over digital networks (including the Internet and wireless networks). However, ICS security is not the only activity in the owner's or operator's cybersecurity portfolio. Compromising a corporate IT system and its connecting networks and information could also bring an organization to a standstill, causing economic damage and jeopardizing the security of the facility and its personnel. As such, an effective cybersecurity framework accounts for threats to both ICSs and corporate IT systems and their connecting networks and information.

The first step in cybersecurity risk management is to identify cyber assets and systems. This step entails identifying and documenting all network infrastructure, devices, applications, data storage, data flows, and all connections to the control systems. Identifying critical cyber assets can be difficult and time-consuming. The cyber supply chain is increasingly complicated, and Critical Manufacturing Sector owners and operators are challenged by identifying the third- or fourth-tier providers whose parts or software are integrated into final products. Common methodologies to support identifying critical cyber assets include those mentioned previously that support identifying critical physical assets: ANSI RA.1-2015, OCTAVE, and FAIR.

Once identified, assets and systems are then assessed. Based on the results of cybersecurity assessments, particular components can be selected for more thorough analysis of cybersecurity vulnerabilities and threats. This is then followed by the implementation of cybersecurity measures through a comprehensive cybersecurity framework. It is important that, throughout all cybersecurity risk management activities, owners and operators remain cognizant of the cyber–physical dependencies and relationships that exist within and connect to their facilities and assets. A successfully implemented cybersecurity framework encompasses information sharing taking place among management and operations personnel operating within the physical and cyber space. This level of information sharing can be achieved through such activities as regular conference calls, cross-discipline working groups, or co-location of personnel.

The Critical Manufacturing Sector is subject to a wide range of risks stemming from cyber threats and hazards. Issues of higher cybersecurity risk for the Critical Manufacturing Sector include ICSs, phishing, intellectual property theft, advanced persistent threat (APT) attacks, distributed denial of service (DDoS) attacks, malware, ransomware, and supply chain attacks. These issues are important for the Critical Manufacturing Sector regarding the cybersecurity of both sector infrastructure and intellectual property.

- **ICSs:** As the Critical Manufacturing Sector advances in technical complexity, increased ICS automation and connectivity introduce new cybersecurity issues. Common high-risk cyber issues of ICSs include exploitation of ICS components (e.g., supervisory control and data acquisition systems, distributed control systems, human–machine interfaces, and programmable logic controllers) through the introduction of malicious code and unauthorized access to ICS components through static, default passwords and malicious website scripting.

- **Phishing:** Cyber threat actors use this strategy to gain access to a target organization's network. The attacker sends a virtual communication (usually an email) to one or more staff members inside the organization, disguising the email's source as a trusted organization or associate. The communication contains a malicious attachment or link. Recognizing the email's source, the recipient opens the attachment or clicks on the link, opening the network to intrusion (e.g., by installing malware or revealing usernames and passwords). Organizations should review their email services and policies to ensure that their security is up to date. All employees and third-party vendors should understand the threat of phishing and know how to handle an email that appears suspicious.
- **Intellectual Property Theft:** Intellectual property is often considered a manufacturer's most valuable asset. The highly competitive, global environment in which the Critical Manufacturing Sector operates is prone to intellectual property theft (especially of research and development data) for illicit gain. Cyberattacks on manufacturers' systems and networks are the predominant method of intellectual property theft in the sector.
- **APT Attacks:** Coordinated long-term cyber campaigns by motivated groups pose significant risk to the Critical Manufacturing Sector. APTs may be able to establish a foothold in a manufacturer's network and move laterally or probe deeper into internal networks undetected to attack ICSs. These types of intrusions can lead to cyber threat actors taking full control of network infrastructure, allowing for further attacks on connected infrastructure (e.g., data theft, espionage, denial of service, or decreased productivity/functionality).
- **DDoS Attacks:** Attacks using many Internet-connected devices are a growing threat. DDoS attacks generate immense bandwidth loads to the point of disruption or create openings for malware to be deployed. As the Critical Manufacturing Sector introduces more Internet-connected devices into its processes, the risk of DDoS attacks also increases. Common security devices that use high-bandwidth connections, such as security cameras and digital video recorders in manufacturing facilities, are of particular concern for DDoS attacks.
- **Malware and Ransomware:** Malware and ransomware are common attacks on all business IT networks and can infect Critical Manufacturing Sector organizations as well. Cyber threat actors may use malware to cause economic and operational damage by altering, corrupting, or stealing data or information; overloading network infrastructure; or creating opportunities for further cyberattacks. Ransomware is a type of malware that cyber threat actors use to deny access to systems or data by encrypting the files and data on the infected computer. Typically, a ransom is demanded by the cyber threat actor to decrypt the data and return functionality. However, paying the ransom may or may not result in the restoration of data or access.
- **Supply Chain Attacks:** Both hardware and software are subject to supply chain attacks through a variety of strategies. For example, cyber threat actors may provide targets with inauthentic or counterfeit hardware, perhaps incorporating covert functionality, or inauthentic software or software components. Attacks may also involve tampering with existing hardware or software. Cyber threat actors can also penetrate systems via vendors who have network connections but who may not have adequate security. Particular attention should be paid when acquiring software or patches to ensure that the source is known and vetted and that the software is verified to be authentic and intact.

Owners and operators may address these or other prominent cybersecurity issues by conducting cybersecurity assessments and implementing cybersecurity measures. Resources that may be helpful for owners and operators to implement cybersecurity measures are listed in Appendix B.

Cybersecurity Framework

As owners and operators rely increasingly on cyber assets and systems, and as cyberattacks become bolder and more sophisticated, the criticality of implementing cybersecurity practices increases. To support cybersecurity assessments and cybersecurity measures, owners and operators are encouraged to adopt a cybersecurity framework, such as the National Institute of Standards and Technology (NIST) *Framework for*

Improving Critical Infrastructure Cybersecurity (Framework). The NIST Framework provides a prioritized, flexible, repeatable, and cost-effective approach to managing cybersecurity risk and can help owners and operators:

- Describe the current cybersecurity posture
- Describe the target state for cybersecurity
- Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process
- Assess progress toward the target state
- Communicate among internal and external stakeholders about cybersecurity risk

The NIST Framework broadly applies across all organizations, regardless of size or cybersecurity sophistication. The Critical Manufacturing Sector developed the *Critical Manufacturing Sector Cybersecurity Framework Implementation Guidance* to help organizations understand and use the Framework as it applies to their particular industry.

Cybersecurity Assessments

The key to robust cybersecurity is to conduct assessments to identify cybersecurity risks and evaluate the organization's cybersecurity practices and cyber operational resilience. For owners and operators, it is important to determine whether an automated control system could be remotely manipulated to cause improper operation and whether improper operation could cause significant damage or destruction. Cybersecurity assessments may be conducted as self-assessments or as onsite assessments facilitated by cybersecurity professionals. By conducting cybersecurity assessments, owners and operators will have a better understanding of their cybersecurity postures, where system vulnerabilities exist, and what actions are required to address them. This empowers owners and operators to prevent or mitigate the consequences of a cyberattack, such as equipment or control systems damage, compromise of corporate IT systems, or manipulation of the security environment. Effective and accepted cybersecurity assessment tools include:

- **Cyber Security Evaluation Tool (CSET)**: Offered by DHS, CSET is a no-cost, voluntary desktop software tool designed to guide users through a step-by-step process to assess their control systems and IT network security practices against recognized industry standards. The user selects one or more of the government- and industry-recognized cybersecurity standards, which will generate assessment questions specific to the selected requirements. The tool then compares completed answers with the recommended requirements from the standards selected. After assessment completion, a prioritized list of recommendations for improving the organization's cybersecurity posture and associated actions to be taken will be made available.
- **Cyber Resilience Review (CRR):** Offered by DHS, the CRR is a no-cost, voluntary, non-technical assessment designed to evaluate an organization's cyber operational resilience and cybersecurity practices across 10 domains. The CRR can be used to evaluate the resilience capabilities of enterprises with highly defined and mature operational resilience capabilities, as well as organizations with less defined and mature capabilities. Owners and operators can also choose to download the free self-assessment or schedule an onsite assessment facilitated by trained DHS cybersecurity professionals; both options generate a final report with options for consideration and the organization's maturity level relative to the assessed domains.

Key resources leveraged by Critical Manufacturing Sector owners and operators to support cybersecurity assessments include:

- ANSI RA.1-2015
- ANSI/ISA-62443 Security for Industrial Automation and Control Systems standard
- Center for Internet Security (CIS) Controls V7
- FAIR
- Information Systems Audit and Control Association (ISACA) Control Objectives for Information and Related Technologies (COBIT) Framework
- ISO/IEC 27000 series standards for IT security
- ISO/IEC 31010 Risk management – Risk assessment techniques standard
- NIST
  - Baldridge Cybersecurity Excellence Builder
  - Special Publication 800-series, Computer Security (including ICSs)
  - Special Publication 1800-series, Cybersecurity Practice Guides
- OCTAVE

Cybersecurity Measures

Effective cybersecurity is achievable only through the implementation of robust and enduring cybersecurity measures organization-wide. To enhance the security of cyber assets and systems, owners and operators can consult the NIST Cybersecurity Framework. The NIST Framework is built from many existing standards, guidelines, and best practices across many industries. It outlines five core cybersecurity functions designed to achieve specific cybersecurity outcomes and references examples of how to achieve those outcomes. This section is organized by the five core functions designed to facilitate cybersecurity risk management: identify, protect, detect, respond, and recover.

Core Functions of the NIST Cybersecurity Framework
Identify: Develop organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities. The activities in the Identify function are foundational for effective use of the Framework.
Protect: Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services. The protect function supports the ability to limit or contain the impact of potential cybersecurity events.
Detect: Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event, enabling the timely discovery of cybersecurity incidents.
Respond: Develop and implement the appropriate activities to take action regarding a detected cybersecurity event. The respond function supports the ability to contain the impact of a potential cybersecurity event.
Recover: Develop and implement the appropriate activities to maintain plans for resilience and restore any capabilities or services impaired by the cybersecurity event.

Identify

NIST Cybersecurity Function: Identify
Asset Management: Identification and management of cyber assets and systems.
Business Environment: The facility's organization, mission, and objectives used to inform cybersecurity roles, responsibilities, and risk management.
Governance: The facility's policies, procedures, and processes used to inform cybersecurity risk.
Risk Assessment: Understanding of cybersecurity risk to operations, assets, and individuals.
Risk Management Strategy: Establishment of priorities, constraints, risk tolerances, and assumptions and their use in risk decisions.
Supply Chain Risk Management: Management of cybersecurity risk associated with external parties relevant to the supply chain.

Similar to other critical infrastructure, Critical Manufacturing Sector facilities employ a variety of ICSs to monitor, automate, and control critical physical processes. Manufacturers also utilize a variety of networks and IT systems with networked information in their daily operations. Identifying these control and IT system assets is critical, as they represent the linchpin for operational facilities. The identification phase involves documenting and evaluating the criticality of the entire network infrastructure, devices, applications, data storage, data flows, and all connections to the cyber assets and systems. For each cyber asset and system, the criticality to the facility's operations is evaluated, and owners and operators may then classify the asset or system as critical or non-critical. When it is more convenient to classify the criticality of the cyber assets as a group, then the criticality of the cyber system as a whole is evaluated instead of the criticality of each individual asset. Cybersecurity measures under the identify function may include identifying and documenting cyber asset vulnerabilities and internal and external threats.

Protect

NIST Cybersecurity Function: Protect
Access Control: Access to assets and facilities is limited to authorized users, processes, or devices.
Awareness and Training: Employees and contractors receive cybersecurity awareness and information security responsibility training.
Data Security: Information and data are managed according to the facility's risk strategy.
Information Protection Processes and Procedures: Security policies are used to manage the protection of information systems and assets.
Maintenance: Maintenance and repair of control systems is performed.
Protective Technology: Technical security solutions are managed to ensure system security and resilience.

Within the Critical Manufacturing Sector, control systems are used either onsite or remotely to control and/or monitor operations. They are subject to issues that complicate their protection: increased connectivity, interdependencies, complexity, legacy systems, wireless connection and communication, offshore reliance, and information availability. In addition to cybersecurity measures protecting control systems, measures need to be in place to prevent or mitigate the various types of cyberattacks, which may be more pervasive than just an attack on control systems. In this phase, protective cybersecurity measures are implemented to protect from several types of cyberattacks: automated cyberattacks (e.g., software attacks from malware), external cyberattacks (e.g., outside individual gaining unauthorized access), or internal cyberattacks (e.g., personnel or contractors/vendors gaining unauthorized access). The criticality determined in the identification phase will decide the level of security measures, such as baseline or enhanced, that should be implemented for the cyber assets or systems. Protective cybersecurity measures may include identifying and credentialing authorized devices and users, remotely managing cyber assets and systems, and employing data loss prevention systems.

Detect

NIST Cybersecurity Function: Detect
Anomalies and Events: Abnormal activity is detected in a timely manner, and potential impact is understood.
Security Continuous Monitoring: Information systems and assets are monitored at distinct intervals.
Detection Processes: Processes and procedures are maintained and tested to ensure timely awareness.

Protective measures may sometimes be insufficient to prevent or mitigate nefarious cyber activity. As such, capabilities to detect cyber intrusion activity, misuse, or negligence are critical to containing the activity and ensuring an appropriate response level. In this phase, detection technology and procedures are implemented to discover abnormal conditions with IT systems and networks using a strategy of continuous monitoring and detection. This function of cybersecurity is intended to enable the ability for rapid response to limit the potential damage of a cyber incident. Embracing a defense-in-depth cybersecurity approach (also referred to as layered protection) includes not only measures to protect against any single point-of-failure types of breaches but also intrusion detection strategies and technology. Cybersecurity detection measures may include establishing and managing a baseline of network operations and expected data flows, conducting regular vulnerability scans, and verifying website certificates and software digital signatures.

Respond

NIST Cybersecurity Function: Respond
Response Planning: Response processes and procedures are executed and maintained.
Communications: Response activities are coordinated with internal and external stakeholders, including law enforcement.
Analysis: Analysis is conducted to ensure adequate response and recovery.
Mitigation: Expansion of the event is prevented, its effects are mitigated, and the incident is eradicated.
Improvement: Facility response activities are improved by incorporating lessons learned from the detection and response phases.

Despite the implementation of cybersecurity measures for protection and detection, a cyber incident compromising asset or facility security may occur. In the event of an incident, the owner or operator seeks to take appropriate action in response to the detected cyber incident. Cybersecurity response activities may include executing a cyber incident response plan and mitigating newly identified vulnerabilities or documenting them as accepted risks. Along with short-term activities specific to the incident recovery phase, a typical response plan might include other processes:

- Determine the nature of the incident.
- Determine whether the incident is malicious or non- malicious in origin.
- Analyze available data sources.
- Respond:
  - Isolate the compromised host.
  - Block malicious traffic with existing security devices.
  - Patch/harden infrastructure to address the specific vulnerability.
  - Report to law enforcement if criminal activity is suspected.
- Recover:
  - Recover the compromised hosts.
  - Survey infrastructure for other vulnerable hosts.
  - Patch/harden as appropriate.
  - Quantify loss if seeking legal remedies.
  - Monitor host and network for signs of subsequent compromise.
  - Conduct post-mortem analysis.

- Revise procedures and training based on post-mortem analysis.

To ensure an effective cyber response, checklists can be developed for teams to respond to various types of cyber incidents. The lists could include other useful information, such as command post locations and instructions for obtaining information updates during the response. In addition, the cyber incident response plan should be reviewed and updated and the response process tested regularly. A tabletop exercise to simulate a cyber incident might be considered.

To establish reliable communications between relevant personnel for a cyber incident, operational technology personnel should understand that cyber incidents can have impacts on operations. Conversely, IT personnel should be aware of vulnerabilities and potential cyber impacts to operational equipment and processes. Effective security programs maintain cyber education across organizational staff who may have a role in cyber incident response. Closer integration between operations and cyber incident response personnel would facilitate a better understanding of how compromised, non-traditional IT devices fit within cyber incident response plans. Since first-line incident responders may work in operations, their ability to classify, escalate, and share incident information with the appropriate cyber incident response teams may affect the speed, and ultimately the quality, of response.

Recover

With the increasing importance of cyber assets and systems to facility operations, rapid recovery is critical to mitigating disastrous effects and maintaining business continuity. In this phase, the owner or operator seeks to restore critical assets and operations to ensure the continued operation of the asset, which might include the execution of recovery plans to bring critical services online quickly. Recovery cybersecurity activities may include executing a recovery plan, managing public relations, and communicating recovery activities to internal stakeholders and executive and management teams. Critical to the recovery phase are post-incident evaluation activities, which may include the following:

NIST Cybersecurity Function: Recover
Recovery Planning: Recovery processes and procedures are executed and maintained.
Improvement: Facility recovery activities are improved by incorporating lessons learned.
Communications: Restoration activities are coordinated with internal and external parties, including coordinating centers, Internet service providers, owners of systems actively attacking, affected systems, other computer security incident response teams, and vendors.

- Collect necessary information/evidence.
- Determine the cause of the incident.
- Determine the effects of the incident.
- Make recommendations for improvements to the systems.
- Make recommendations for improvements to the incident response.

Personnel Security Practices

The effectiveness of all Critical Manufacturing Sector security operations—including those for physical, cyber, or personnel—is dependent on the people who perform and manage such efforts throughout the sector each day. Owners, operators, personnel, and contractors all perform mission-critical tasks to implement security measures and maintain mission integrity. Such high levels of responsibility necessitate appropriately high levels of scrutiny, training, and education because the errant or illicit actions of one person can cause catastrophic damage to assets, facilities, and sector organizations.

Assessing personnel threats includes screening potential and new hires or contractors for specific security risk criteria, periodically rescreening personnel, and determining the likelihood of, and vulnerability to, insider threats. The results of these activities inform owner and operator decisions on implementing personnel security measures such as background investigations, training to increase security awareness and education, and exercises and drills to hone skills and knowledge related to specific types of security incidents. Though not explicitly associated with personnel security risks and incidents, the development and management of response and recovery plans are included in this chapter as important drivers of personnel functions applicable to all-hazards incidents.

The threat of malicious insiders is the major personnel security issue of concern for Critical Manufacturing Sector owners and operators.

- **Insider Threat:** The insider threat can be described as an insider using his or her authorized access, wittingly or unwittingly, to do harm to the organization's resources, personnel, facilities, information, equipment, networks, or systems. Insiders may be employees, former employees, business partners, contractors, consultants, temporary personnel, interns, or vendors. Insiders often have knowledge of a facility's security features, which could be used to circumvent security measures in order to disrupt operations. An insider may be a hardworking, trusted employee for many years before deciding to attack his or her own organization. As a result, the insider threat may be the most difficult threat to identify and mitigate prior to an attack.

Owners and operators may address this or other prominent personnel security issues by conducting personnel security assessments and implementing personnel security measures.

Personnel Security Risk Assessments

Risk assessment for personnel security within the Critical Manufacturing Sector is primarily focused on the risks posed by existing or potential personnel to the secure operation and maintenance of facilities and assets. Major portions of common risk assessment practices regarding sector personnel include screening potential hires and existing personnel (employees and contractors) for risk factors in individuals' characteristics and history, periodic rescreening of personnel for the same risk factors using a screening program, and examining the potential for deliberate malicious activity by personnel. The results of such assessments can be used to inform decisions about personnel and hiring changes, as well as to identify areas in which new or additional personnel security measures may be warranted.

Screen and Rescreen

Many owners and operators develop effective hiring policies that include an initial background screening to evaluate a potential candidate's character, employment qualifications, and fitness for the position being sought. A background screening can also be used to investigate any potential hiring risks for safety and security reasons. Typically, such screening includes items such as past employment verifications, criminal history, and credit checks. The position being sought, the level of security required, and the access to critical assets and operations will determine the appropriate level of screening. Sector owners and operators may

choose to develop a standard program for all personnel screening and rescreening to provide consistency, track information over time, and eliminate any potential for discrimination or prejudice. Basic elements of an effective personnel screening program may include:

- Consistent use of a standard application form or specialized forms, as site specifics warrant
- A definitive and rigidly enforced policy regarding which applicants must complete certain forms and background checks
- A clearly stated and consistently enforced policy that failure to agree to a required background check will result in rejection of the application
- A clearly outlined process for receiving applications, reviewing them for completeness, making acceptance or rejection decisions, documenting the decisions, and maintaining records of them
- Precise definitions of any terms used to designate differing levels of access to facility equipment, buildings, records, computer systems, and control systems
- Background check procedures and questions that comply with applicable federal and/or state laws, any union agreements, and organization policy
- Trained individuals to adjudicate investigative results and make decisions or recommendations regarding hiring of individual applicants
- Standardized acceptance and rejection form letters
- Clearly stated criteria for which applications will be rejected
- A precisely stated appeals process for rejected applicants

Properly screening personnel may help mitigate some risk to the organization; however, screening does not eliminate all risks and threats posed by vetted personnel and contractors.

Assess Insider Threat

Insider incidents may account for billions of dollars, annually, in lost revenue, according to a well-recognized source for insider threat data.[1] Malicious actions result in losses such as thefts of trade secrets, deliberate destruction of computer systems, and damage to an organization's reputation once the loss is made public. The risk occurs regardless of organization size and location. Many organizations do not see themselves as vulnerable, but a life's work on a unique design or piece of software can be stolen and transferred out of the country in a few minutes. Disgruntled or former employees can act slowly (for example, bleeding data away for years) or swiftly (for example, destroying the organization's systems). The impacts are devastating and spill over into communities in the form of lost jobs and opportunities. In some instances, entire industries and research efforts have been lost to overseas competitors who used those secrets to build rival firms. Sensitive national security programs are put at risk, as well, when components, parts, design plans, and specialized equipment are stolen. Assessing threats of malicious insiders is imperative in light of such potential impacts.

An effective program for assessing personnel in terms of insider threats may include:

- Procedures to properly evaluate personnel and contractor information, including consultation with the facility's or organization's legal counsel, human resources, and civil liberties and privacy officials to ensure compliance with all applicable laws and privacy requirements

[1] National Counterintelligence and Security Center, National Insider Threat Task Force, *Protect Your Organization from the Inside Out: Government Best Practices* (2016)

- Compliance assessments of personnel regarding insider threat policies and procedures to ensure the program is working as intended
- A process to facilitate the sharing of information from human resources, intelligence, law enforcement, and other pertinent sources to recognize the presence of an insider threat

Appropriate measures to mitigate insider threats uncovered by personnel risk assessments are provided in the following Personnel Security Measures section. Key resources leveraged by Critical Manufacturing Sector owners and operators to support personnel security risk assessments (including insider threat assessments) include:

- ASIS International Preemployment Background Screening Guideline 2009
- Carnegie Mellon University Software Engineering Institute Common Sense Guide to Mitigating Insider Threats
- Carnegie Mellon University Software Engineering Institute Open Source Insider Threat (OSIT) Information Sharing Working Group
- CTPAT Personnel Screening
- DHS Chemical Facility Anti-Terrorism Standards (CFATS) Personnel Surety
- DOD Insider Threat Program Best Practices
- DOD Procedures for the DOD Personnel Security Program (Manual 5200.02)
- Executive Order 13587: National Insider Threat Policy
- National Counterintelligence and Security Center National Insider Threat Task Force (NITTF) Insider Threat Guide 2017
- NITTF Insider Threat Program Maturity Framework 2018

Personnel Security Measures

Effective practices for personnel security in the Critical Manufacturing Sector, commensurate with personnel risk assessments, generally adhere to the fundamental risk management concepts of prevent and prepare, detect and assess, delay and deny, and respond and recover. Owners and operators conduct background investigations, training, and exercises, as well as incorporate lessons learned (from past incidents, training, and exercises), to better prepare personnel for security incidents and potentially prevent some incidents from occurring at all. Security awareness training, insider threat considerations, and standardized suspicious activity reporting are all effective means for detecting and assessing existing or potential personnel security incidents.

Physical security measures identified in the Physical Security Practices chapter to delay and deny an adversary's progress through a facility are also relevant for supporting personnel security. Response and recovery planning, including BCPs, EAPs, and recovery plans—bolstered with a commonly understood and observed incident management and command structure—give owners and operators clear pathways and procedures to maximize effective response and recovery and minimize incident consequences to facilities, assets, and communities.

Prevent and Prepare

Large-scale emergency incidents at Critical Manufacturing Sector facilities are not common events. Therefore, training and exercises are necessary to maintain operational readiness, timeliness, and responsiveness. In addition, effective training and exercises may prevent personnel-caused security incidents. If such incidents do occur, clearly documenting and incorporating lessons learned from the incidents enhances the capability of sector owners, operators, and other personnel to prevent similar incidents from occurring again.

- **Procedural Considerations:** When applicable, owners and operators may choose to develop procedures to require segregation of duties or delegation of authority for the operation of critical assets so that one employee does not control the entire process for critical operations. This will ensure continuity of critical operations in emergency situations, resulting in the temporary or permanent loss or incapacitation of key personnel, and will reduce the probability of personnel error in critical functions. The DHS Business Continuity Suite provides guidance on such procedural considerations.
- **Training:** The proper training of personnel and contractors/vendors is critical to the success of every organization. Training provides personnel with the knowledge, skills, and abilities to effectively perform key tasks to better accomplish the organizational mission. Owner/operator security training decisions can be based on information compiled from assessments, planning, and operations while using best industry practices as guidelines. Including baseline security awareness training is a means of instilling a common culture of security awareness among personnel. More detail on security awareness training is provided below in the Detect and Assess portion of this section. Well-informed and well-aware personnel may be able to recognize situations or conditions that have the potential to lead to a security incident and take corrective actions to prevent the incident from occurring.
- **Exercises:** The development and execution of exercises and drills in preparation for potential security incidents is a critical factor in determining the effectiveness of the overall security measures of a facility. Through exercises, organizations validate security plans, test operational capabilities, assess leadership effectiveness, and examine the various ways to prepare and respond to incidents. Essential exercise-related activities include preparing the exercise, managing exercise activities, and conducting immediate wrap-up activities such as lessons learned. To assist the owner or operator in preparing for and managing exercises and drills, DHS has implemented the Homeland Security Exercise and Evaluation Program (HSEEP). HSEEP offers a common exercise policy and provides program guidance that constitutes a national standard for exercises. HSEEP includes consistent terminology that can be used by all exercise planners, regardless of the nature and composition of their sponsoring agency or organization. This program offers useful tools that exercise managers can use to plan, conduct, and evaluate exercises to improve overall preparedness.
- **Lessons Learned:** Documenting and leveraging past information regarding incidents and exercises is an important way to better prepare for future events or potentially prevent certain types of incidents from happening. Capturing lessons learned and creating an archive is an effective method for developing and improving a site's security posture. Understanding what went right and wrong may greatly reduce the chances of repeating past mistakes. Sector owners and operators often develop formal, documented lessons learned processes that are updated as needed to capture this critical information. Formal meetings are also employed to discuss, capture, document, and share lessons learned after each incident or exercise. The meetings may include many topics, such as successes and why they were successful; failures and why they occurred; processes that should be kept, revised, or discarded; and what processes or actions could have been improved (e.g., efficiency, costs, protection, or response). The focus of these efforts is to capitalize on past successes or failures to improve a facility's overall security.

Detect and Assess

To appropriately identify and evaluate personnel security risks and incidents, owners and operators commonly combine general security awareness training, insider threat policies and measures, and suspicious activity reporting.

- **Security Awareness Training:** Security awareness training is based on the need to inform personnel (including contractors) of security risks and their specific responsibilities for complying with security policies and procedures. It is important that training requirements be set and documented for every

employee and contractor, as the needs may vary based on each individual's role and responsibilities. Major subject areas for security awareness training commonly include cybersecurity, physical security, insider threat, terrorism and criminal activity, workplace violence, and active shooter. Prominent examples of security awareness training programs are listed in Appendix B. Key areas for consideration when developing a security awareness training program include:

  - Require annual (at a minimum) security awareness training and testing.
  - Maintain a central location for training resources and documentation.
  - Define total annual hours of training required per position type and responsibilities.
  - Develop incentive programs for training compliance and innovation.
  - Implement visitor security awareness requirements, as appropriate.

- **Insider Threat Policies:** Critical Manufacturing owners and operators understand the importance of detecting insider threats and assessing personnel actions and behaviors for the potential of insider threats. Standardized and documented insider threat identification and evaluation policies and procedures may reduce the probability of an insider attack as well as minimize the length of time between insider threat detection and mitigation. Effective approaches to detecting and assessing insider threats include technological monitoring and auditing of personnel access control (e.g., movement through controlled doors, locks, and barriers) and computer network use for activities or patterns of activity that may indicate an insider threat. Also, owners and operators may choose to implement an integrated, centralized reporting and response program to detect and mitigate insider threats. This program may include the protocols and required documentation for investigating allegations of insider threats, all of which are approved by the organization's legal counsel, human resources, security management, and civil liberties and privacy officials.
- **Suspicious Activity Reporting:** Communication with personnel and vendors about security concerns and suspicious activities is crucial to overall facility security. The acknowledgment of a suspicious activity may be the first indication that a malicious illicit event may occur. Therefore, owners and operators may choose to develop and implement a method for employees and trusted vendors or contractors to report security-related incidents and suspicious activity. The Homeland Security Information Network – Critical Infrastructure (HSIN-CI) Suspicious Activity Reporting Tool for critical infrastructure owners and operators allows HSIN-CI users to submit formalized reports of suspicious activity within their communities to sector leadership and government agencies.
- **Delay and Deny:** Sector personnel may employ physical security measures to delay the advancement of an adversary or deny the adversary's access to sensitive areas or assets in a facility or an organization's networks. It is important to consider that some established personnel safety measures may conflict with physical security measures. The Physical Security Measures section of the Physical Security Practices chapter provides delay and deny examples of entry control components, electronic access control systems, and barriers.

Respond and Recover

The close coordination of a facility's personnel in the aftermath of a security incident is imperative for effective response and recovery. The actions taken by personnel after an incident has occurred can make the difference between minor consequences and major catastrophes. As a result, owners and operators readily employ extensive planning for incident response and recovery. A common type of response plan across the sector is the EAP. Recovery plans are also prominently featured and are often included within an EAP. These plans provide a consistent, commonly understood structure and process by which sector personnel can take corrective and mitigation actions. Personnel safety and security is paramount during an incident, and so response and recovery plans commonly include stipulations for maintaining personnel safety during egress or evacuation from an incident. Roles and responsibilities of specific personnel, including specialized response or recovery teams, are a major component of response and recovery plans,

which typically include portions relating to federal incident management guidance such as the National Incident Management System (NIMS) and its Incident Command System component.

- **National Incident Management System:** NIMS provides a proactive approach to systematically assist all levels of government, utility providers, and private-sector organizations to work seamlessly in response to incidents. The NIMS approach is effective for any situation that involves coordination among multiple agencies or partners. The goal is to coordinate activities to reduce consequences (loss of life, property damage, and harm to the environment). The Incident Command System is a core element of NIMS and is composed of a standardized, on-scene, all-hazards incident management approach that allows for the integration of personnel, procedures, facilities, equipment, and communications operating within a common organizational structure. The Incident Command System also enables a coordinated response among jurisdictions and agencies, in both the public and private sectors. Further, it establishes common processes for planning and managing resources and proper budgetary allocations. Owners and operators may incorporate NIMS and Incident Command System information into an EAP and/or a recovery plan. This allows all users to easily reference the needed information in a single location.
- **Emergency Action Planning:** An EAP is a formal document that identifies potential emergency conditions at a facility and specifies actions to be followed to minimize loss of life and property damage. The EAP typically contains the information necessary to guide owners and operators in preventing, responding to, and mitigating impending incidents and minimizing any ensuing life safety consequences and property damage. Common elements worth considering for an EAP include (but are not limited to):
  - Actions the facility owner will take, in coordination with emergency management authorities, to mitigate a problem, risk, or emergency incident at the facility
  - Procedures owners will follow to provide early warning and notification to responsible downstream emergency management authorities
  - Delineation of the responsibilities of all those involved in managing an incident or emergency and how the responsibilities should be coordinated and communicated

  Annual EAP exercises and annual reviews and updates of the EAP—as well as the subcomponent plans it may contain (e.g., recovery, security, and/or evacuation plans)—are valuable means to maintain the EAP's relevance and effectiveness of associated response and recovery policies and procedures.

- **Recovery Planning:** The establishment of a recovery plan can help to minimize incidents' potential impacts, including downtime and economic consequences. These plans detail the processes and information the owner or operator needs to efficiently and effectively respond to many adverse events. Recovery plans enable owners and operators to more quickly mitigate, recover, and reinstate essential services and functions. A recovery plan differs from an EAP in that it is more specifically focused on the response and recovery aspects of an event. Typically, the EAP covers a much more robust set of documentation spanning a very wide spectrum of emergency situations. Common elements shared by EAPs and recovery plans include processes and protocols for defined types of emergency scenarios, an incident command system with assignment of responsibilities, coordination with local authorities, and primary and backup communications equipment. Other common elements include drawings, maps, and photographs of facilities and assets to aid in response; sources and availability of vehicles, equipment, materials, supplies, and contractors; and estimated response times per incident type.
- **Response and Recovery Teams:** Response and recovery plans may indicate response and recovery measures in accordance with the type and severity of incident. For some incidents, specifically defined teams of personnel may be called upon to perform the measures deemed necessary. Personnel may include local law enforcement or an onsite security force. Owners and operators

should routinely coordinate and collaborate with local law enforcement to facilitate adequate understanding of the facility and mission, as well as security threats. Owners and operators may also consider appointing a recovery team to plan and oversee the long-term recovery process. The team would include members experienced with evaluation of structures, systems, equipment, and operations; if necessary, these teammates can develop alternative approaches (subject to owner approval) for returning to normal operations quickly and safely.

Supply Chain Security Practices

The Critical Manufacturing Sector relies heavily on complex, effective global and domestic supply chains to deliver raw goods, manufactured parts, and final components. With rising international commerce, manufacturers' supply chains have grown more extensive, complex, and interdependent—involving potentially hundreds of facilities, vendors, and suppliers, in as many regions. A global web of transportation pathways, IT, and cyber and energy networks has created supply chain efficiencies that enable just-in-time shipments and reduced inventories, but this same network can hinder the ability to absorb disruptions. This interconnected, interdependent network can allow supply chain disruptions in the Critical Manufacturing Sector to cascade across wide geographic regions and industries, threatening the economy and national security.

Important issues of concern for Critical Manufacturing Sector organizations regarding supply chain security and resilience include introduction of counterfeit parts and components, geopolitical issues such as conflict and crime, globalization affecting the pricing and availability of products and raw materials, and concentration or bottlenecking at coastal ports.

- **Counterfeiting:** 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.
- **Geopolitical Issues:** Availability of materials may be affected by geopolitical disturbances in areas identified as conflict zones. Procurement and delivery or raw materials originating from such areas are subject to disruption by armed conflict and regulation. Crime-afflicted areas of the world that coincide with major manufacturing contribute additional risk to sector operations and supply chains. In addition, political issues endemic to specific countries or regions can greatly influence the cost of doing business in those areas.
- **Globalization:** International events could have significant and unpredictable impacts on domestic manufacturing, including pricing, availability, and delivery of products and raw source materials. Significant delays or closures at a single port (e.g., from a natural disaster) can have widespread consequences, and labor disputes or bilateral policy issues can involve more than one site.
- **Geographical Concentration:** Concentration of Critical Manufacturing Sector facilities around coastal ports could magnify geographic issues and the effects of local disasters and labor disruptions. Significant delays or closures at a single port can have widespread consequences, and labor disputes or bilateral policy issues can involve more than one site.

Owners and operators may address these and any other prominent supply chain issues by conducting supply chain security risk assessments and implementing supply chain security measures.

Supply Chain Security Risk Assessments

Critical Manufacturing Sector organizations continuously enhance their operations through strategies such as globalization, outsourcing, off-shoring, specialized manufacturing, supply base rationalization, just-in-time deliveries, supplier consolidation, and lean inventories. While these strategies offer many benefits in efficiency and effectiveness, they also render supply chains increasingly prone to risk and can increase the likelihood of supply chain disruptions. Such risks inherent in the current manufacturing operating environment necessitate the employment of supply chain risk assessments for security and resilience. An organization's approach to supply chain risk assessment should be tailored to meet its needs, context of operation, risk tolerance, and unique supply chain characteristics. Supply chain risk assessments generally include supply chain risk identification, the analysis of those risks, and the evaluation of risk analysis results.

- **Supply Chain Risk Identification:** Actions to identify supply chain risks may include brainstorming sessions, referencing previous risk assessments (for physical, cyber, or personnel security), conducting surveys, conducting business impact analyses (see Appendix E for a sample business impact analysis worksheet), or other efforts to identify and list potential risks within the organization's supply chain processes. The table below provides examples of different types of supply chain risks that manufacturers may consider. In addition, supply chain risk identification may include the following considerations:
  - Number and location of suppliers
  - Number and origin of shipments
  - Contractual terms defining security requirements for supplier or vendor shipments
  - Modes of transport (e.g., air, surface, rail, barge, or marine) and routes for shipments
  - Other logistics providers or partners involved in the supply chain (e.g., packaging companies, warehousing, trucking companies, freight forwarders, and air or ocean carriers) that handle shipments

Potential Supply Chain Risks	
External Risks	
Natural disasters	Labor unavailability
Industrial accidents	Market challenges
Sabotage, terrorism, crime, war	Lawsuits
Political uncertainty	Technological trends
Supplier Risks	
Physical and regulatory risks	Management risks
Production problems	Upstream supply risks
Financial losses and premiums	
Distribution Risks	
Infrastructure unavailability	Lack of capacity
Labor unavailability	Cargo damage or theft
Warehouse inadequacies	IT system inadequacies or failure
Long, multi-party supply pipelines	
Internal Enterprise Risks	
Operational	Political uncertainty
Demand variability	Personnel availability
Design uncertainty	Planning failures
Financial uncertainty	Facility unavailability
Testing unavailability	Enterprise underperformance
Supplier relationship management	

- **Supply Chain Risk Analysis:** Risks identified as relevant to the supply chain should be comparatively analyzed to estimate the likelihood and consequences of their occurrence. These supply chain risks then may be accordingly prioritized for mitigation. Organizations may choose to rank risk events based on an overall qualitative risk level. However, such a simplistic approach should be used only as an initial analysis to rapidly prioritize identified risks and select those that should receive immediate attention. Detailed analysis of the likelihood and consequences of supply chain risks may be conducted to generate more quantitative results. For example, risk likelihood could be analyzed based on five-point scales of percentages (e.g., from less than 5 percent for the least probable to more than 90 percent for the most probable) and consequences (e.g., from less than 2 percent of

gross revenue for the least economic impact to more than 20 percent of gross revenue for the greatest economic impact) for a numerical result.

- **Supply Chain Risk Evaluation:** After conducting a supply chain risk analysis, the results can be evaluated for acceptable levels of risk, or risk tolerance. Acceptable risk levels will be unique to each organization and supply chain. The levels may vary by commodity, product, or service, as well as over time. Different risk-tolerance levels may be set for different levels of the organization. While generally tied to financial impact, through which risks may best be understood and compared, risks may also be tied to other corporate assets such as reputation. One method of evaluating risk is to use a "heat-map" showing risk events on a matrix defining likelihood and consequence levels. This technique allows managers to examine the relative likelihood and consequence of differing risks. To use this method effectively, it is critical to have well-defined and consistently used criteria for the different likelihood and consequence levels. An example of a heat map is included in Appendix G.

Key resources to support supply chain risk assessment for Critical Manufacturing Sector owners and operators include:

- ANSI/ASIS Supply Chain Risk Management: A Compilation of Best Practices (SCRM.1-2014)
- CTPAT Five-Step Risk Assessment
- ISO 31010 Risk management – Risk assessment techniques standard
- ISO/IEC 28000 series standards for supply chain security
- NIST Cybersecurity Framework
- NIST Supply Chain Risk Management Practices for Federal Information Systems and Organizations (SP-800-161)
- Supplier Compliance Audit Network (SCAN) audits
- Supply Chain Risk Leadership Council Supply Chain Risk Management: A Compilation of Best Practices

Supply Chain Security Measures

Supply chain security practices seek to anticipate, prevent, protect, mitigate, manage, respond to, and recover from potentially undesirable and disruptive events. An organization's approach to such events is determined by its context of operations, its tolerance of different levels of supply chain risk, and the results of supply chain risk assessments. Effective practices for supply chain security in the Critical Manufacturing Sector, commensurate with supply chain risk assessments, generally adhere to the fundamental risk management concepts of prevent and prepare, detect and assess, and respond and recover.

Prevent and Prepare

Supply chain risk management succeeds when effective practices and policies are included in pragmatic plans that are accessible, adhered to, and adaptive. Comprehensive planning allows organizations to prevent disruptions from occurring, or adapt effectively when they do occur. Planning also allows organizations to continue to reap the benefits of innovations in supply chain risk management after their value has been demonstrated. Effective supply chain risk management planning includes modernizing risk management plans for increased automation, mitigation, and simulation; adapting security controls during emergency events to address short-term risks; and incorporating cyber supply chain risk management in planning.

- **Modernizing Risk Management Plans:** Supply chain risk management—and the plans that govern it—must be flexible to remain relevant in a dynamic risk environment. Organizations that are modernizing their plans for supply chain risk management are increasing provisions for automation, such as replacing older software and equipment with streamlined and automated processes to

reduce legacy system risk. Current and future risk mitigation activities should be selected by weighing the difficulty of their execution versus the level of risk. Such analysis can be used to adapt planning as risks evolve and new risks arise. Similarly, innovative organizations are using simulation to modernize their risk management plans—such as testing the business continuity plans of first-tier suppliers for effectiveness in simulated disruptive events—and adjusting plans accordingly.

- **Adapting Security Controls During Emergency Events:** Major disruptive events, such as natural disasters, can force companies to adjust acquisition procedures to compensate for limited component availability or other supplier-based difficulties. One consequence can be increased opportunity for counterfeit components to infiltrate the supply chain. An effective planning strategy to mitigate counterfeiting during natural disasters is to increase security control measures (e.g., component or supplier monitoring, screening, or authorization) along the affected supply chain while the disruption persists. After the disruption ends, organizations can reinstate normal, steady-state security controls.
- **Incorporating Cyber Supply Chain Risk Management:** Cyber supply chain risk management is the set of activities necessary to manage cybersecurity risk associated with external parties. More specifically, cyber supply chain risk management addresses both the cybersecurity effect an organization has on external parties and the cybersecurity effect external parties have on an organization. A primary objective of cyber supply chain risk management is to identify, assess, and mitigate products and services that may contain potentially malicious functionality, are counterfeit, or are vulnerable as a result of poor manufacturing and development practices within the cyber supply chain. Cyber supply chain risk management activities may include:
  - Determining cybersecurity requirements for suppliers
  - Enacting cybersecurity requirements through formal agreement (e.g., contracts)
  - Communicating to suppliers how those cybersecurity requirements will be verified and validated
  - Verifying that cybersecurity requirements are met through a variety of assessment methodologies
  - Governing and managing the above activities

Detect and Assess

Supply chain analysis and assurance are essential portions of effective supply chain risk management. These important activities involve monitoring the multitude of information associated with—and auditing points or components along—the supply chain to characterize, quantify, and qualify its operation. This close supervision allows owners and operators to effectively detect and assess security threats or events in the supply chain. Examples of best practices for monitoring and auditing include developing real-time situational awareness tools for supply chain tracking and tracing, identifying counterfeit types relevant to the supply chain, establishing centralized security operations centers for continuous supply chain analysis, and automating supply chain mapping, supplier assessment, and process notification.

- **Developing Real-Time Situational Awareness Tools:** The ability to effectively mitigate supply chain risks is founded on timely awareness of potential disruptions. Advance notice of a failure, delay, or emergency allows for proactive mitigation measures to be taken. Developing tools that operate in real time to provide information on the status of parts, products, or processes is a common method of enhancing supply chain monitoring and auditing. Recent advancements in such tools provide transparency of supplier production rates and causes of failure, visibility into a part or component's provenance to reduce counterfeit risk, historical data to support auditing of processes, and cybersecurity analysis of networks and data to identify anomalies.
- **Identifying Counterfeit:** Identifying types of counterfeiting threats can help to inform appropriate mitigations, such as adopting industry anti-counterfeit standards and best practices, developing a

trusted supplier network, including audits in supplier contracts, and establishing documented policies and procedures for employees to follow when counterfeit is discovered. Several general types of counterfeit may be considered:

  - Adulterate: A component of the legitimate finished product is fraudulent.
  - Tamper: Legitimate product and package are used in a fraudulent way.
  - Overrun: Legitimate product is made in excess of production agreements.
  - Theft: Legitimate product is stolen and passed off as legitimately procured.
  - Diversion: Legitimate product is sold or distributed outside of intended markets.
  - Simulation: Illegitimate product is designed to look like but not exactly copy the legitimate product.
  - Complete counterfeit: All aspects of the fraudulent product and package are fully replicated.

- **Establishing Centralized Security Operations Centers:** Maintaining the security of vastly distributed assets, networks, processes, suppliers, and personnel within supply chains can be exceedingly complex. Owners and operators may alleviate the complexity by establishing centralized hubs of security management for cyber and physical security. These centers enable continuous remote monitoring and controlling of access to company facilities and networks. Similarly, establishing central, collaborative auditing communities for real-time supply chain risk management enhances the organization's ability to rapidly detect and assess supply chain threats or anomalies.
- **Automating Supply Chain Mapping, Supplier Assessment, and Process Notification:** Advances in supply chain risk management drive organizations to expand and enhance monitoring and auditing, leading to ever-increasing amounts of information. The data deluge, in turn, effects a need for data management. Automated solutions exist or may be created to address monitoring and auditing information needs, and leading companies are leveraging automation to execute, manage, and streamline supply chain mapping, supplier assessment, and process notification. Automated systems map the entire supply chain at multiple tiers and can track every part or component, including its manufacturing, testing, shipping, and distribution. Additional automation can be linked with supply chain mapping to increase efficiencies and situational awareness through supplier assessments (e.g., for business continuity plans and corporate responsibility requirements) and process notifications (e.g., parts changes, fabrication rates, and component lead times). These solutions are valuable not only for collecting and analyzing all the incoming data but also for visually presenting the analyzed data for rapid assessment of the supply chain.

Respond and Recover

Despite even the best preparation, planning, and situational awareness, Critical Manufacturing Sector owners and operators will confront supply chain security incidents. Such incidents can create unstable supply chain conditions that require urgent attention and action to protect life, assets, property, operations, income, the environment, and/or reputation. Effective supply chain incident response often involves intense time constraints, high levels of stress, and the need for rapid yet careful decision making. Planning for and implementing crisis management processes are important components of effective supply chain incident response and recovery. Crisis management comprises the overall strategic and tactical responses of an organization to recognize and respond effectively, efficiently, and comprehensively to supply chain incidents.

Crisis management processes are intended to enhance existing response capabilities by establishing a crisis-management structure that will provide integrated and coordinated planning and response activities at all levels within an organization. The structure and processes are designed to complement, yet not supersede, emergency response plans and procedures at various functional organization units and facilities.

- **Crisis Management Team:** For supply chain incidents, a crisis management team may be activated to assess the incident, define the risks, and develop the appropriate response operations. The team

may manage the response through briefings and communications with senior staff, customer service personnel, and others as needed. The team resolves the incident once a clear path is established to restore operations to normal capacity.

- **Recovery:** Depending on the severity of the supply chain incident, recovery could span hours, days, weeks, or longer. Returning operations to a normal state should be supported by business continuity planning, as described in the Physical Security Practices chapter. For supply chain incident recovery, business continuity planning should include information on who needs to act, what mitigations need to be enacted, and when actions need to be completed to help resume normal operations.

Appendix A. Resources

Key resources for this document are listed below in alphabetical order within each chapter topic.

Physical Security Practices

American National Standards Institute (ANSI), Risk Assessment Standard, https://webstore.ansi.org/standards/asis/ansiasisrimsra2015

ASIS International, Facilities Physical Security Measures Guideline, https://www.asisonline.org/publications/sg-asis-facilities-physical-security-measures-guideline-2009-ed/

Carnegie Mellon University Software Engineering Institute, Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process, https://resources.sei.cmu.edu/asset_files/TechnicalReport/2007_005_001_14885.pdf

Department of Defense (DOD), Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs, https://www.acq.osd.mil/se/docs/2017-rio.pdf

DHS, National Terrorism Advisory System (NTAS), www.dhs.gov/alerts

DHS, Risk Lexicon, http://www.dhs.gov/dhs-risk-lexicon

DOD, Unified Facilities Criteria (UFC) Electronic Security Systems, https://www.wbdg.org/FFC/DOD/UFC/ufc_4_021_02_2013.pdf

DOD, UFC Emergency Operations Center Planning and Design, https://www.wbdg.org/FFC/DOD/UFC/ufc_4_141_04_2008_c1.pdf

DOD, UFC Entry Control Facilities/Access Control Points, https://www.wbdg.org/FFC/DOD/UFC/ufc_4_022_01_2017.pdf

DOD, UFC Minimum Antiterrorism Standards for Buildings, https://www.wbdg.org/FFC/DOD/UFC/ufc_4_010_01_2018.pdf

DOD, UFC Security Engineering Facilities Planning Manual, https://www.wbdg.org/FFC/DOD/UFC/ufc_4_020_01_2008.pdf

DOD, UFC Security Engineering: Physical Security Measures for High-Risk Personnel, https://www.wbdg.org/FFC/DOD/UFC/ufc_4_010_03_2011.pdf

DOD, UFC Security Fences and Gates, https://www.wbdg.org/FFC/DOD/UFC/ufc_4_022_03_2013.pdf

International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), Risk management – Risk assessment techniques, https://www.iso.org/standard/51073.html

The Open Group, Factor Analysis of Information Risk (FAIR), https://www.opengroup.org/forum/security-forum-0/risk-management

Transported Asset Protection Association (TAPA) Facility Security Requirements (FSR), https://tapa.memberclicks.net/assets/docs/Standards/2017-Standards/tapa_fsr_2017_final%20march%202017.pdf

U.S. Customs and Border Patrol, Customs Trade Partnership Against Terrorism (CTPAT) Five Step Risk Assessment, https://www.cbp.gov/sites/default/files/documents/C-TPAT%27s%20Five%20Step%20Risk%20Assessment%20Process.pdf

Cybersecurity Practices

ANSI, Risk Assessment Standard, https://webstore.ansi.org/standards/asis/ansiasisrimsra2015

ANSI, Security for Industrial Automation and Control Systems standard, https://www.isa.org/templates/one-column.aspx?pageid=111294&productId=116731

Carnegie Mellon University Software Engineering Institute, Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process, https://resources.sei.cmu.edu/asset_files/TechnicalReport/2007_005_001_14885.pdf

Center for Internet Security (CIS), Controls V7, https://www.cisecurity.org/controls/

DHS, Critical Manufacturing Sector Cybersecurity Framework Implementation Guidance, https://www.dhs.gov/sites/default/files/publications/critical-manufacturing-cybersecurity-framework-implementation-guide-2015-508.pdf

Information Systems Audit and Control Association (ISACA), Control Objectives for Information and Related Technologies (COBIT) Framework, http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx

ISO/IEC, 27000 Series standards – Information security management systems, https://www.iso.org/isoiec-27001-information-security.html

ISO/IEC, 31010 Risk Management – Risk Assessment Techniques standard, https://www.iso.org/standard/51073.html

National Institute of Standards and Technology (NIST), Framework for Improving Critical Infrastructure Cybersecurity, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

NIST, Special Publication 1800-series, Cybersecurity Practice Guides, https://www.nist.gov/itl/nist-special-publication-1800-series-general-information, https://csrc.nist.gov/publications/sp1800

NIST, Special Publication 800-series, Computer Security, https://www.nist.gov/itl/nist-special-publication-800-series-general-information, https://csrc.nist.gov/publications/sp800

The Open Group, FAIR, https://www.opengroup.org/forum/security-forum-0/risk-management

Personnel Security Practices

ASIS, Preemployment Background Screening Guideline, https://www.asisonline.org/publications/sg-asis-preemployment-background-screening-guideline-2009-ed/

Carnegie Mellon University Software Engineering Institute, Common Sense Guide to Mitigating Insider Threats, https://resources.sei.cmu.edu/asset_files/TechnicalReport/2016_005_001_484758.pdf

Carnegie Mellon University Software Engineering Institute, Open Source Insider Threat (OSIT) Information Sharing Working Group, https://insights.sei.cmu.edu/insider-threat/2017/11/announcing-the-national-insider-threat-center.html

CBP, CTPAT Personnel Screening, https://www.cbp.gov/sites/default/files/documents/pss.pdf

DHS, Chemical Facility Anti-Terrorism Standards (CFATS) Personnel Surety, https://www.dhs.gov/cisa/cfats-personnel-surety-program, https://www.dhs.gov/sites/default/files/publications/csat-psp-instructions-508-2_0.pdf

DHS, Homeland Security Exercise and Evaluation Program (HSEEP), https://preptoolkit.fema.gov/documents/1269813/1269861/HSEEP_Revision_Apr13_Final.pdf/65bc7843-1d10-47b7-bc0d-45118a4d21da

DOD, Procedures for the DOD Personnel Security Program, https://www.esd.whs.mil/portals/54/Documents/DD/issuances/dodm/520002_dodm_2017.pdf

National Counterintelligence and Security Center (NCTC), National Insider Threat Task Force (NITTF) Insider Threat Guide, https://www.dni.gov/files/NCSC/documents/nittf/Insider-Threat-Guide-2017-one-page-view(032618).pdf

NCTC, NITTF Insider Threat Program Maturity Framework, https://www.dni.gov/files/NCSC/documents/nittf/20181024_NITTF_MaturityFramework_web.pdf

NCTC, NITTF Protect Your Organization from the Inside Out: Government Best Practices https://www.dni.gov/files/NCSC/documents/products/Govt_Best_Practices_Guide_Insider_Threat.pdf

The White House, Executive Order 13587: National Insider Threat Policy, https://www.dni.gov/files/NCSC/documents/nittf/National_Insider_Threat_Policy.pdf

Supply Chain Security Practices

ANSI/ASIS, Supply Chain Risk Management: A Compilation of Best Practices, https://webstore.ansi.org/standards/asis/ansiasisscrm2014

CBP, CTPAT Five Step Risk Assessment, https://www.cbp.gov/sites/default/files/documents/C-TPAT%27s%20Five%20Step%20Risk%20Assessment%20Process.pdf

ISO, 28000 Series standards – Specification for security management systems for the supply chain, https://www.iso.org/standard/44641.html

ISO/IEC, 31010 Risk management – Risk assessment techniques standard, https://www.iso.org/standard/51073.html

NIST, Framework for Improving Critical Infrastructure Cybersecurity, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

NIST, Supply Chain Risk Management Practices for Federal Information Systems and Organizations, https://csrc.nist.gov/publications/detail/sp/800-161/final

Supplier Compliance Audit Network, Improving Supply Chain Audit Efficiencies through Collaboration,

http://www.scanassociation.com

Supply Chain Risk Leadership Council, Supply Chain Risk Management: A Compilation of Best Practices, http://www.scrlc.com/articles/Supply_Chain_Risk_Management_A_Compilation_of_Best_Practices_final%5B1%5D.pdf

Appendix B. Tools, Training, and Programs

Below is a list of relevant tools, training, and programs that may help Critical Manufacturing Sector stakeholders implement security practices described in this document. These resources are organized by alphabetical order within each chapter topic. This listing is not exhaustive, but it provides key resources sector stakeholders may find useful.

Physical Security Practices

Active Shooter Preparedness Program – DHS maintains a comprehensive set of resources and in-person and online trainings that focus on behavioral indicators, potential attack methods, how to develop emergency action plans, and the actions that may be taken during an incident. https://www.dhs.gov/active-shooter-preparedness

Business Continuity Planning Suite – This DHS suite is designed to be user-friendly and scalable for optimal organizational use to reduce the potential impact of a business disruption. The Suite includes business continuity planning training, business continuity and disaster recovery plan generators, and a business continuity plan validation. http://www.ready.gov/business-continuity-planning-suite

Chemical Security Assessment Tool (CSAT) – This DHS online portal houses the surveys facilities must submit so DHS can determine which facilities are considered high-risk under the Chemical Facility Anti-Terrorism Standards (CFATS). CSAT houses surveys and applications for the Top-Screen, Security Vulnerability Assessment (SVA), Site Security Plan (SSP), and Personnel Surety Program (PSP). https://www.dhs.gov/cisa/chemical-security-assessment-tool

Counter-IED Training and Awareness – OBP develops tools to improve national preparedness for bombing threats at all levels of government, for the public, and within the private sector. Course options include bombing prevention workshops, soft target awareness, and surveillance detection. https://www.dhs.gov/publication/bombing-prevention-training-fact-sheet

Counter-Improvised Explosive Device (IED) Awareness Products – The Office of Bombing Prevention (OBP) provides a wide array of awareness products—including cards, posters, checklists, guides, videos, briefings, and applications—that share counter-IED awareness information with the general public and across the public and private sectors to prevent, protect against, respond to, and mitigate bombing incidents. https://www.dhs.gov/counter-ied-awareness-products

Disaster Recovery Institute International (DRI International) Professional Practices for Business Continuity Management: This framework assists owners and operators in developing, implementing, and maintaining business continuity programs and plans. The framework also can serve as a means for assessing the business continuity capabilities of an organization and identify gaps and opportunities for improvement. https://drii.org/resources/professionalpractices/EN

Homeland Security Information Network (HSIN) – HSIN is a national, secure, trusted Web-based portal for information sharing and collaboration between federal, state, local, tribal, territorial, private sector, and international partners engaged in the homeland security mission. HSIN provides secure, real-time collaboration tools, including a virtual meeting space, instant messaging, and document sharing to allow partners to work together instantly, regardless of their location, to communicate, collaborate, and coordinate. HSIN is also a valuable resource for the cybersecurity, personnel, and supply chain security practices in this document. https://www.dhs.gov/homeland-security-information-network-hsin

Infrastructure Survey Tool (IST) – The IST is a voluntary web-based security survey conducted by a DHS Protective Security Advisor in coordination with facility owners and operators to identify a facility's overall security and resilience. https://www.dhs.gov/cisa/infrastructure-survey-tool

Protective Security Advisor (PSA) Program – CISA PSAs are security subject matter experts who engage with state, local, tribal, and territorial (SLTT) government mission partners and private-sector stakeholders to protect the Nation's critical infrastructure. PSAs serve as a link to DHS infrastructure protection resources; coordinate vulnerability assessments, training, and other DHS products and services; facilitate information sharing in steady state and incident response; and assist facility owners and operators with obtaining security clearances.

Ready Business – The DHS Ready Business program helps businesses develop a preparedness program by providing tools to create a plan that addresses the impacts of many hazards. This website and its tools utilize an "all-hazards approach" and follow the program elements within National Fire Protection Association 1600, Standard on Disaster/Emergency Management and Business Continuity Programs. https://www.ready.gov/business

U.S. Customs and Border Patrol (CBP) Customs Trade Partnership Against Terrorism (CTPAT) – Through this program, CBP works with the trade community to strengthen international supply chains and improve U.S. border security; in exchange, CBP affords CTPAT partners certain benefits, including reduced examination rates and access to the Free and Secure Trade (FAST) lanes. https://www.cbp.gov/border-security/ports-entry/cargo-security/ctpat

Cybersecurity Practices

Automated Indicator Sharing (AIS) – The CISA AIS capability enables the exchange of cyber threat indicators (e.g., malicious internet protocol [IP] addresses or the sender address of a phishing email) between the Federal Government and the private sector at machine speed. https://www.us-cert.gov/ais

Critical Infrastructure Cyber Community (C3) Voluntary Program Small and Midsize Business (SMB) Toolkit – To help business leaders get started, DHS has provided a list of top resources specially designed to help SMBs recognize and address their cybersecurity risks. https://www.us-cert.gov/sites/default/files/c3vp/smb/Top_SMB_Resources.pdf

Critical Manufacturing Sector Cybersecurity Framework Implementation Guidance – This DHS guidance document was developed to help Critical Manufacturing Sector owners and operators use the voluntary National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity. https://www.dhs.gov/publication/critical-manufacturing-cybersecurity-framework-implementation-guidance

Cyber Essentials – This CISA guide and website helps leaders of small businesses as well as leaders of small and local government agencies to develop an actionable understanding of where to start implementing organizational cybersecurity practices. https://www.cisa.gov/sites/default/files/publications/19_1106_cisa_CISA_Cyber_Essentials_S508C_0.pdf, https://www.cisa.gov/cyber-essentials

Cyber Resilience Review (CRR) – The CRR is a no-cost, voluntary, non-technical assessment to evaluate an organization's operational resilience and cybersecurity practices. The CRR may be conducted as a self-assessment or as an on-site assessment facilitated by DHS cybersecurity professionals. The CRR assesses enterprise programs and practices across a range of ten domains, including risk management, incident management, service continuity, and others. https://www.us-cert.gov/ccubedvp/assessments#Downloadable%20Resources

Cyber Security Evaluation Tool (CSET) – CSET is a DHS product that helps organizations protect their key national cyber assets. This desktop software tool guides users through a step-by-step process to assess their control system and IT network security practices against recognized industry standards. https://www.us-cert.gov/ics/Assessments

Cybersecurity Advisor (CSA) Program – CISA CSAs assist with preparing and protecting private-sector entities and SLTT governments from cybersecurity threats. CSAs play an essential engagement and outreach role through their direct interactions with sector stakeholders affected by a cybersecurity incident. CSAs promote cybersecurity preparedness, risk mitigation, and incident response capabilities, working to engage stakeholders through partnership and direct assistance activities.

Cybersecurity for Small Businesses – This 30-minute, self-paced training exercise from the Small Business Administration provides an introduction to securing information in small businesses. https://www.sba.gov/tools/sba-learning-center/training/cybersecurity-small-businesses

Enhance Email & Web Security – This CISA four-page flyer describes practices to improve cybersecurity for an organization's email and web services and includes links to resources with more guidance and tools. https://www.cisa.gov/sites/default/files/publications/CISAInsights-Cyber-EnhanceEmailandWebSecurity_S508C.pdf

Federal Communications Commission Small Biz Cyber Planner – This planner helps businesses create custom cybersecurity plans and includes information about cyber insurance, advanced spyware, and how to install protective software. https://www.fcc.gov/cyberplanner

Federal Trade Commission: Protecting Small Businesses – This small business website helps business owners avoid scams, protect their computers and networks, and keep their customers' and employees' data safe. https://www.ftc.gov/about-ftc/bureaus-offices/bureau-consumer-protection/small-businesses

Federal Virtual Training Environment (Fed VTE) – FedVTE is a free online, on-demand cybersecurity training system that is available at no charge for government personnel and veterans. Managed by DHS as part of the National Initiative for Cybersecurity Careers and Studies, FedVTE contains more than 800 hours of training on topics such as ethical hacking and surveillance, risk management, and malware analysis. https://niccs.us-cert.gov/training/federal-virtual-training-environment-fedvte

Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) Monitor –CISA provides a newsletter as a service to personnel actively engaged in the protection of critical infrastructure assets. https://www.us-cert.gov/ics/monitors

Industrial Control Systems Cybersecurity Training – CISA ICS program training events consist of regional training courses and workshops at venues in various locations, in addition to a five-day training event held monthly in Idaho Falls, Idaho. https://www.us-cert.gov/ics/Training-Available-Through-ICS-CERT

Industrial Control Systems Private-Sector Critical Infrastructure Assessments – CISA provides cybersecurity assessments in partnership with critical infrastructure owners and operators to strengthen the cybersecurity posture of their ICSs. https://www.us-cert.gov/ics/Assessments

Internet Essentials for Business 2.0 – This guide from the U.S. Chamber of Commerce for business owners, managers, and employees focuses on identifying common online risks, best practices for securing networks and information, and what to do when a cyber incident occurs. https://www.uschamber.com/CybersecurityEssentials

National Initiative for Cybersecurity Careers and Studies (NICCS) Education and Training Catalog – This catalog is a central location of over 3,000 cybersecurity related courses from over 125 different providers. The catalog can be searched by course location, preferred delivery method (e.g., online or in-person), specialty area, and proficiency level. Courses are designed for participants to add a skillset, increase their level of expertise, earn a certification, or transition to a new career. https://niccs.us-cert.gov/training/search

Network Security Training – CERT Network Security Training provides technical staff members, engineers, software managers, and technical leads best practices and practical techniques for protecting the security of their organization's information assets and resources. https://www.cert.org/training/

NIST Baldridge Cybersecurity Excellence Builder – This self-assessment tool helps organizations better understand the effectiveness of their cybersecurity risk management efforts and identify improvement opportunities in the context of their overall organizational performance. https://www.nist.gov/baldrige/products-services/baldrige-cybersecurity-initiative

NIST Framework for Improving Critical Infrastructure Cybersecurity – This voluntary Framework consists of standards, guidelines, and best practices to manage cybersecurity-related risk. The Cybersecurity Framework's prioritized, flexible, and cost-effective approach helps to promote the protection and resilience of critical infrastructure and other sectors important to the economy and national security. https://www.nist.gov/cyberframework

NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide – This publication helps organizations establish computer security incident response capabilities and handle incidents efficiently and effectively. It provides guidelines for incident handling, particularly for analyzing incident-related data, and determining the appropriate response to each incident. The guidelines can be followed independently of particular hardware platforms, operating systems, protocols, or applications. https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final

Stop.Think.Connect. Toolkit – The Stop.Think.Connect. campaign has an online Toolkit that includes information specific to SMBs. https://www.dhs.gov/stopthinkconnect-toolkit

Strategic Partnership Programs – Strategic Partnership Coordinators in Federal Bureau of Investigation (FBI) field offices can help businesses or academic institutions protect their technologies and prevent significant economic and national security losses. https://www.fbi.gov/file-repository/counterintelligence-strategic-partnership-programs.pdf

FBI InfraGard – InfraGard is a partnership between the FBI and members of the private sector. The InfraGard program provides a vehicle for seamless public–private collaboration with government that expedites the timely exchange of information and promotes mutual learning opportunities relevant to the protection of critical infrastructure. https://www.infragard.org/

U.S. Secret Service Electronic Crimes Task Forces (ECTFs) – ECTFs prevent, detect, and investigate various forms of electronic crimes, including cybercrime. ECTFs rely on trusted partnerships between the law enforcement community, the private sector, and members of academia to combat cybercrime through information sharing, coordinated investigations, technical expertise, and training. https://www.secretservice.gov/data/investigation/USSS-Cyber-Investigations-Flyer.pdf

Understanding Digital Signatures – This CISA Security Tip describes software digital signatures and how they work to secure and safeguard the integrity of software and data. https://www.us-cert.gov/ncas/tips/ST04-018

Understanding Website Certificates – This CISA Security Tip describes website certificates and encryption and how to check a website's certificate. https://www.us-cert.gov/ncas/tips/ST05-010

White Paper: Every Small Business Should Use the NIST Cybersecurity Framework – This white paper from eManagement can help SMBs understand and use the NIST Cybersecurity Framework. It provides cybersecurity tips for SMBs aligned to the Framework's core functions: Identify, Protect, Detect, Respond, and Recover. https://cyber-rx.com/wp-content/uploads/2015/08/CyberRx-white-paper_SBs-should-use-NIST-CS-Framework_FINAL-20150804.pdf

Personnel Security Practices

Economic Espionage Campaign – The link provides information about the FBI nationwide awareness campaign for economic espionage. https://www.fbi.gov/news/stories/economic-espionage

Homeland Security Exercise and Evaluation Program (HSEEP) – This DHS program provides a set of guiding principles for security exercise programs, as well as a common approach to exercise program management, design and development, conduct, evaluation, and improvement planning. https://preptoolkit.fema.gov/web/hseep-resources

Insider Threat project – The DHS Science and Technology Directorate (S&T) Insider Threat project develops solutions that complement and expand capabilities of existing commercial insider threat tools and furthers insider threat research. https://www.dhs.gov/science-and-technology/csd-insider-threat

IS-906: Workplace Security Awareness – This FEMA course provides guidance to individuals and organizations on how to improve security in the workplace. https://training.fema.gov/is/courseoverview.aspx?code=IS-906

IS-907: Active Shooter: What You Can Do – This FEMA course provides guidance to individuals, including managers and employees, so that they can prepare to respond to an active shooter situation. https://training.fema.gov/is/courseoverview.aspx?code=IS-907

IS-914: Surveillance Awareness: What You Can Do – The purpose of this FEMA course is to make critical infrastructure employees and service providers aware of actions they can take to detect and report suspicious activities associated with adversarial surveillance. https://training.fema.gov/is/courseoverview.aspx?code=IS-914

IS-915: Protecting Critical Infrastructure against Insider Threats – This FEMA course provides guidance to critical infrastructure employees and service providers on how to identify and take action against insider threats to critical infrastructure. https://training.fema.gov/is/courseoverview.aspx?code=IS-915

IS-916: Critical Infrastructure Security: Theft and Diversion – What You Can Do – This FEMA course introduces critical infrastructure personnel to the information they need and the resources available to them to identify threats and vulnerabilities to critical infrastructure from the theft and diversion of critical resources, raw materials, and products that can be used for criminal or terrorist activities. https://training.fema.gov/is/courseoverview.aspx?code=IS-916

Risk Assessment & Insider Threat Training – CERT Risk Assessment & Insider Threat training teaches managers, executives, security and business continuity professionals, risk managers, compliance personnel, and insider threat program managers to develop strategies for protecting their organizations from security threats and to better manage their risks. Topics covered include the CERT Resilience Management Model (CERT-RMM), OCTAVE Allegro method, and insider threat program management best practices. https://www.cert.org/training/

Spotting Insider Threats Guide – This FBI Office of the Private Sector guide defines insider threats and lists what to do when such threats are discovered. https://www.fbi.gov/file-repository/spotting-insider-threat_508.pdf

Suspicious Activity Reporting Tool – The DHS Homeland Security Information Network – Critical Infrastructure (HSIN-CI) Suspicious Activity Reporting Tool allows non-uniformed, private-sector law enforcement members to submit formalized suspicious activity reports and facilitate efficient information sharing and responsiveness. https://www.dhs.gov/suspicious-activity-reporting-tool

Supply Chain Security Practices

Academy of Aerospace Quality (AAQ) Counterfeit Parts Course – This online course outlines the effects and impacts of counterfeit parts, as well as how different organizations address the problem. http://aaq.auburn.edu/counterfeit-parts

American Bearing Manufacturers Association (ABMA) Customs Education Seminar – ABMA offers this training opportunity to help government law enforcement improve customs enforcement against counterfeit bearings. https://www.americanbearings.org/page/anti_c_domestic

Electric Power Research Institute (EPRI) Training – EPRI offers this nuclear-industry-specific training that includes modules describing counterfeit, fraudulent, and substandard items; identifying the risks they present; and describing actions that can be implemented to reduce risk. https://www.epri.com/#/pages/product/1020955/?lang=en

Overseas Security Advisory Council (OSAC) – OSAC promotes security cooperation between U.S. private-sector interests worldwide and the U.S. Department of State. OSAC's information-exchange website offers the latest in safety- and security-related information, public announcements, warden messages, travel advisories, significant anniversary dates, terrorist group profiles, country crime and safety reports, special topic reports, foreign press reports, and much more. https://www.osac.gov/Pages/Home.aspx

U.S. Department of Defense, Defense Acquisition University – DOD offers this series of guidebooks, best practices, and training courses on counterfeit parts. https://www.dau.mil/acquipedia/Pages/ArticleDetails.aspx?aid=5ea0eba7-13f0-40be-9ec7-0e1fa52934ad

U.S. Nuclear Regulatory Commission (NRC) Counterfeit, Fraudulent, Suspect Item Training Offerings – U.S. NRC Information Notice 2012-22 lists training opportunities for education and awareness on counterfeit, fraudulent, or suspect components. https://www.nrc.gov/docs/ML1231/ML12318A216.pdf

Appendix C. Elements of Criticality

Critical Manufacturing Sector owners and operators may evaluate business assets and functions for criticality using the matrix below. There are six impact categories and five levels of impact per category ranging from not applicable to severe. A business asset, function, process, or program is deemed "critical" if it includes a business process meeting a medium threshold (when that process is unavailable for 30 days). A business impact analysis may be conducted to determine how quickly a critical program needs to be recovered in order to avoid unacceptable impacts to the company.

Impacts	N/A	Low	Medium	High	Severe
Financial	Impact does not apply	Revenue loss less than *[$xxx]* and/or cash flow decrease less than *[$xxx]*	Revenue loss between *[$xxx]* and/or cash flow decrease between *[$xxx]*	Revenue loss between *[$xxx]* and/or cash flow decrease between *[$xxx]*	Revenue loss between *[$xxx]* and/or cash flow decrease between *[$xxx]*
Customer Service and Support		Minimal disruption or degradation of service and support, but not at a scale that would impact customer confidence	Moderate disruption or degradation of service and support at a scale that impacts customer confidence in the short term	Strong disruption of service and support causing some long-term loss of customer confidence, possible loss of customers, and adverse media attention	Severe disruption of service and support causing long-term loss of customer confidence and resulting in probable loss of customers and adverse media attention
Reputation		Minimal impact to company reputation but not perceivable to anyone outside of the business	Moderate impact to company reputation in the short term	Strong impact to company reputation with long-term business implications	Severe impact to company reputation with permanent damage to business stability
Production		Disruption of less than *[xxxx]*	Disruption of *[xxxx]*	Disruption of *[xxxx]*	Disruption of more than *[xxxx]*
Contractual		Minimal short-term impact to meeting contractual obligations	Moderate impact to meeting contractual obligations, possible impact to customer relationship in the short term	Strong impact to meeting contractual obligations affecting long-term customer relationship with potential liability exposure and/or performance penalties	Severe impact to meeting contractual obligations resulting in loss of customer and future business with liability exposure and/or performance penalties
Legal/Regulatory		Possibility of indirect legal and/or regulatory impacts	Activity governed by legal and/or regulatory requirements with possibility of small to moderate fines	Activity governed by legal and/or regulatory requirements with possibility of high fines and temporary suspension of operating license	Activity governed by legal and/or regulatory requirements with possibility of prolonged or sustained suspension of operating license and/or criminal charges

Appendix D. Sample Security Plan Outline

The following is a sample outline of a security plan to assist owners or operators in developing a security plan for their specific sites.

1. INTRODUCTION, PURPOSE AND SCOPE

2. APPLICABILITY, DEFINITIONS AND RESPONSIBILITIES
    - 2.1 Applicability
    - 2.2 Definitions
    - 2.3 Designated Personnel Responsibilities
        - 2.3.1 Incident Commander
        - 2.3.2 Security Coordinator
        - 2.3.3 Risk Coordinator
        - 2.3.4 Corporate Communications Coordinator
        - 2.3.5 Other positions as required

3. SITE DESCRIPTION

4. OPERATIONAL PROCEDURES
    - 4.1 General Security Guidelines
    - 4.2 Security Personnel
    - 4.3 General Access Requirements
    - 4.4 Prohibited Items
    - 4.5 Weapons
    - 4.6 Key Control
    - 4.7 Information Protection

5. RESTRICTED AREAS

6. CRITICAL ASSET LIST AND DESCRIPTIONS

7. PHYSICAL SECURITY FOR CRITICAL ASSETS
    - 7.1 Purpose
    - 7.2 Responsibilities
    - 7.3 Physical Security Descriptions, Layout and Inventory
    - 7.4 Physical Security Standards and Administration
    - 7.5 Access Controls
    - 7.6 Reception Lobbies and Other Entry Points
    - 7.7 Electronic Access Controls
    - 7.8 Securing Computers
    - 7.9 Securing Desktop Computers
    - 7.10 Securing Laptop Computers
    - 7.11 Protecting Sensitive Information
    - 7.12 Protection of Sensitive Data
    - 7.13 Use of Courier Services to Ship Sensitive Information
    - 7.14 Protection of Security System Servers
    - 7.15 Security Check Process
    - 7.16 Access Control, Intrusion & CCTV System Maintenance
    - 7.17 Key Control Program
    - 7.18 Access Card Maintenance

Appendix E. Business Impact Analysis Worksheet

The following table can be used as a worksheet for owners and operators to conduct business impact analyses on assets or functions.

Department / Function / Process _____

Operational & Financial Impacts

Timing / Duration	Operation Impacts	Financial Impact

Considerations (customize for your business)

Timing: Identify point in time when interruption would have greater impact (e.g., season, end of month/quarter, etc.)

Duration: Identify the duration of the interruption or point in time when the operational and or financial impact(s) will occur.

- < 1 hour
- >1 hr. < 8 hours
- > 8 hrs. <24 hours
- > 24 hrs. < 72 hrs.
- > 72 hrs.
- > 1 week
- > 1 month

Operational Impacts

- Lost sales and income
- Negative cash flow resulting from delayed sales or income
- Increased expenses (e.g., overtime labor, outsourcing, expediting costs, etc.)
- Regulatory fines
- Contractual penalties or loss of contractual bonuses
- Customer dissatisfaction or defection
- Delay executing business plan or strategic initiative

Financial Impact

Quantify operational impacts in financial terms.

Appendix F. Cybersecurity Checklist

The following is a general cybersecurity checklist of considerations and practices for a manufacturing facility.

Culture of Security	
☐	Software security policies and code of conduct are established in corporate-level policy.
☐	The software development process includes security requirements that align with applicable cybersecurity standards such as ISO 27034, NIST 7622, NIST 800-53, or equivalent.
☐	Secure coding standards are established in company policies and verified through a secure code validation process.
☐	Supplier demonstrates appropriate cybersecurity training and awareness of and adherence to all corporate security policies.
☐	Software developers have performance metrics that track the degree to which cybersecurity objectives are met (e.g., adherence to Mitre top "N" - CWEs).
Technical Security	
☐	Remote or unauthorized access to the source code repository is not allowed by policy.
☐	Supplier ensures adequate cybersecurity skills for assigned software developers and other relevant technical personnel.
☐	Testing and assessment methodologies verify compliance with secure coding standards appropriate to the level of product criticality.
☐	Known vulnerabilities such as common weakness enumeration (CWE) and common vulnerabilities and exposures (CVEs) are evaluated by automated and manual testing.
☐	The supplier actively participates in industry forums such as SAFECODE or the Software Assurance Forum or similar initiatives to ensure familiarity with current threats.
Software Development Life Cycle (SDLC) Security Elements	
☐	Your company identifies, assesses, and mitigates cybersecurity threats throughout the SDLC for all applications and patch releases.
☐	The development environment used in the creation of software includes cybersecurity controls and code security analysis (e.g., SANS Critical Security Controls).
☐	Supplier ensures that software releases, including updates, are free from significant levels of security defects (6 or higher on the NIST Common Vulnerabilities Scoring System, or equivalent).
☐	Delivered software has no hard-coded passwords or default access capabilities.
☐	Development artifacts (e.g., debug code) are removed from production code.
☐	Supplier includes cybersecurity considerations within the supplier's established configuration management process.
☐	Supplier demonstrates effective cybersecurity intrusion and integrity protections for the development environment.

Supply Chain Security	
☐	Supplier discloses the pedigree of all software components used in the product, including any outsourced software components, commercial off-the-shelf (COTS) components, open-source software, or reused components.
☐	Supplier has a risk assessment program that manages cyber risk from its supply chain.
☐	Supplier requires software vulnerability testing on sub-tier supplier software.
☐	Supplier identifies any outsourced software vulnerability testing.
☐	Supplier does not outsource software patch development.
☐	Supplier does not outsource software compilation and/or distribution.
Internal Audits	
☐	Independent audits of all software releases for compliance with company security standards are conducted.
☐	Independent audits for compliance with security policies are conducted on a defined and risk-driven schedule.
☐	Audit results drive changes in the implementation of the SDLC.
Notification, Response, and Recovery	
☐	Supplier has a process for monitoring for emerging threats and vulnerabilities and conducting impact assessment for supplier products.
☐	Supplier prepares a causal analysis to determine the root cause of security vulnerabilities.
☐	Supplier notifies owner/operator of security vulnerabilities and their impact on supplier software or that of sub-tiers.
☐	Supplier prepares a response and a recovery plan for impacted customers, affected operations, and other stakeholders.
☐	Supplier maintains a business continuity/resilience plan that includes cybersecurity and disaster recovery.

Appendix G. Sample Risk Assessment Heat Map

Owners and operators often evaluate risk in terms of a "heat map" that shows risk events in a matrix defining likelihood and criticality levels. This technique allows facility managers to easily see the relative likelihood and consequence of differing risks. To use this method effectively, it is critical to have well-defined and consistently used criteria for the different likelihood and criticality levels.