COMMERCIAL FACILITIES SECTOR

Cybersecurity Framework Implementation Guidance

MAY 2020

U.S. Department of Homeland Security
Cybersecurity and Infrastructure Security Agency

Table of Contents

Introduction

The National Institute of Standards and Technology (NIST) Cybersecurity Framework provides a policy framework of computer security guidance for how private sector organizations in the United States can assess and improve their ability to prevent, detect, and respond to cyberattacks.[1] It can be used to help identify and prioritize actions for reducing cybersecurity risk, and it is a tool for aligning policy, business, and technological approaches to managing that risk. Different types of entities—including sector coordinating structures, associations, and organizations—can use the Framework for different purposes.

In 2018, NIST released Version 1.1 of the Framework for Improving Critical Infrastructure Cybersecurity. The update encourages maturity in cybersecurity assessments and the vulnerability disclosure process, outlines an expanded scope of identity management and access control, and provides supply chain risk management guidance to help mitigate risks associated with industrial control systems and connected devices.[2]

The Commercial Facilities Sector embraces the flexibility the Framework offers. The Cybersecurity and Infrastructure Security Agency (CISA) within the Department of Homeland Security (DHS), as the Sector-Specific Agency, worked with the Commercial Facilities Sector Coordinating Council (SCC) and Government Coordinating Council (GCC) to develop this Implementation Guidance.

[1] National Institute of Standards and Technology (NIST), "Cybersecurity Framework," Updated June 13, 2018, https://www.nist.gov/cyberframework.
[2] Thu Pham, "Updated NIST Cybersecurity Framework Emphasizes Access Control & Supply Chain Risk," Decipher, May 3, 2018, https://duo.com/decipher/updated-nist-cybersecurity-framework-emphasizes-access-control-and-supply-chain-risk.

Framework Overview and Benefits

The United States depends on the reliable functioning of critical infrastructure. Cybersecurity threats exploit the increased complexity and connectivity of critical infrastructure systems, placing the Nation's security, economy, and public safety and health at risk. Similar to financial and reputational risks, cybersecurity risk affects a company's bottom line. It can drive up costs and affect revenue, potentially harming an organization's ability to innovate and gain and maintain customers. Cybersecurity can be an important and amplifying component of an organization's overall risk management.[3] The basics of cybersecurity include the following:

- **Passwords:** Factory-set passwords should not be used and should instead be immediately made unique. Passwords are best when they possess a high level of complexity and are changed periodically. They should also be further protected through multi-factor authentication.
- **Configuration Management Programs:** Software should be protected through validated patches and by routinely applying updates. Any unused ports should be locked down and secured.
- **Cyber Hygiene:** An organization should host mandatory cybersecurity training, create lockout policies, revoke ex-employees' login information, and whitelist software to promote a secure level of cyber hygiene.

Cybersecurity threats can take a variety of forms, all of which endanger the vitality and resilience of critical infrastructure. Malicious actors may implement many tactics to breach an organization, resulting in myriad negative outcomes including, but not limited to, loss of privacy, data, money, and life, disruption of service, and depreciation of consumer confidence. These tactics include:

- **Distributed Denial-of-Service Attack**: A malicious and coordinated flood of web traffic that shuts down a site for a prolonged period of time.
- **Malware**: Harmful software distributed through a computer's system (often requiring the user to take an action, such as clicking on an email attachment.) Examples of malware include "viruses, worms, malicious mobile code, Trojan horses, rootkits, spyware, and some forms of adware."[4]
    - **Ransomware**: A type of malware that encrypts data that can only be unlocked when ransom is paid.[5]
    - **Trojan Horse**: A malicious program disguised as, or embedded within, legitimate software that will install itself and run automatically once downloaded.
    - **Virus**: A program that infiltrates and infects a computer. A virus can corrupt, disseminate, or delete data once established on a computer.[6]
- **Man-in-the-Middle Attack**: An interruption into a two-party transaction that allows attackers to filter and steal data during the transaction.
- **Pharming**: A means of directing users to a malicious or illegitimate website by redirecting the original uniform resource locator (URL).

---

[3] National Institute of Standards and Technology (NIST), *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1, April 16, 2018, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.
[4] National Institute of Standards and Technology (NIST), "Cybersecurity Basics: Glossary," https://www.nist.gov/itl/smallbusinesscyber/cybersecurity-basics/glossary.
[5] Ibid.
[6] Ibid.

- **Phishing**: Fraudulent emails, text messages, or websites purporting to be from a trusted source that require action, such as sending money or confidential documents to the "source."[7]
    - **Spear Phishing**: A highly targeted phishing attack.[8]
- **SQL Injection**: Malicious code that injects a server and forces it to disclose private data.
- **Watering Hole Attack**: An attack that involves corrupting a highly trafficked website, so that a user's computer is also infected when visiting the corrupt website.

To better address these risks, the Cybersecurity Enhancement Act of 2014[9] (CEA) updated the role of NIST to include identifying and developing cybersecurity risk frameworks for voluntary use by critical infrastructure owners and operators. In 2014, NIST released Version 1.0 of the Framework for Improving Critical Infrastructure Cybersecurity to provide a structure that organizations, regulators, and customers can use to create, guide, assess or improve comprehensive cybersecurity programs.[10]

Version 1.1 of the Framework, released in 2018, refines, clarifies, and enhances Version 1.0. Updates include clarification of terms; a section on self-assessment; an expanded explanation of how to use the Framework for cyber supply chain risk management applications; refined language for authentication, authorization, and identity proofing; an improved explanation of the relationship between the implementation tiers and the profiles; and a new subcategory concerning vulnerability disclosures. Version 1.1 can be implemented by first-time and current Framework users, with minimal or no disruption.[11]

The Framework provides a common mechanism for organizations to:

1) describe their current cybersecurity posture,
2) describe their target state for cybersecurity,
3) identify and prioritize opportunities for improvement within the context of a continuous and repeatable process,
4) assess progress toward the target state, and
5) communicate among internal and external stakeholders about cybersecurity risk.

The Framework offers a flexible way to address cybersecurity. It is applicable to organizations relying on technology, including information technology (IT), industrial control systems (ICS), cyber-physical systems (CPS), or connected devices including the Internet of Things (IoT). It complements, but does not replace, an organization's risk management process, cybersecurity program, or related framework implementation; every organization must decide how to individually implement the Framework. The Framework can aid organizations in addressing cybersecurity as it affects the privacy of customers, employees, and other parties. It may also serve to assist suppliers that perform physical work on mission-critical equipment (e.g., software updates, firmware replacement, equipment maintenance, refurbishments, and replacements). Additionally, the Framework's outcomes serve as targets for workforce development and evolution activities.

Potential Benefits of Implementing the Framework

[7] Ibid.
[8] Ibid.
[9] *See* 15 U.S.C. § 272(e)(1)(A)(i). The Cybersecurity Enhancement Act of 2014 (S.1353) became public law 113-274 on December 18, 2014 and may be found at: https://www.congress.gov/bill/113th-congress/senate-bill/1353/text.
[10] National Institute of Standards and Technology (NIST), *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.0, February 12, 2014.
[11] National Institute of Standards and Technology (NIST), *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1, April 16, 2018, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

Choosing to implement the Framework means that an organization wishes to take advantage of the benefits that the Framework offers; it does not imply that an existing cybersecurity and risk management approach is ineffective or needs to be replaced.[12] Specifically, implementing the Framework provides a mechanism for an organization to:

- assess and specifically **describe its current and targeted cybersecurity posture**;
- **identify gaps** in its current programs and processes;
- identify and **prioritize opportunities for improvement** using a continuous and repeatable process;
- **assess progress** toward reaching its target cybersecurity posture;
- **demonstrate the organization's alignment** with nationally recognized best practices;
- highlight any current practices that might **surpass the Framework's recommended practices**; and
- **communicate its cybersecurity posture in a common, recognized language** to internal and external stakeholders—including customers, regulators, investors, and policymakers.

NIST designed the Framework to provide a nationally recognized approach to cyber risk management using best practices and proven processes. As more sectors and organizations implement the Framework, its approach will serve as an accepted baseline for cybersecurity practices in critical infrastructure organizations. Early adoption of the Framework's principles may better position Commercial Facilities Sector organizations to receive additional potential benefits in the future:

- **More attractive cybersecurity insurance coverage:** As cyber risks grow, insurance agencies are developing new and refined approaches to evaluate clients' premiums based on their use of sound cybersecurity practices. Framework implementation provides an additional, widely accepted means for an organization to measure its cybersecurity posture and demonstrate continuous improvement.
- **Availability of technical assistance:** The Federal Government provides several hands-on tools that will help an organization assess their current state of cybersecurity practices and identify areas to grow their cybersecurity resilience. In particular, Cybersecurity Advisors (CSAs) offer assistance to help prepare State, local, tribal, and territorial governments and private sector entities from cybersecurity threats. For more information about CSA technical assistance or to identify your CSA, please email cyberadvisor@cisa.dhs.gov.
- **Demonstration of commitment to cybersecurity:** The Framework does *not* protect any organization from liability in the event of a cyber incident. However, implementation of the Framework provides an organization with a mechanism to demonstrate its proven track record of implementing and continuously evaluating cyber risk management practices appropriate for its individual risks.
- **Government recognition:** For interested organizations, DHS seeks to recognize those organizations and sectors – regardless of size and maturity level – that use the Framework to enhance their risk management practices.
- **Workforce development:** Organizations that use the Framework will have a better understanding of the technical capabilities their organization requires and, therefore, the skills required of their cyber workforce such as recruiting, workforce design, and training of existing personnel.

Risk Management and the Framework

[12] U.S. Department of Energy (DOE) Office of Electricity Delivery and Energy Reliability, *Energy Sector Cybersecurity Framework Implementation Guidance*, January 2015, https://www.energy.gov/sites/prod/files/2015/01/f19/Energy%20Sector%20Cybersecurity%20Framework%20Implementation%20Guidance_FINAL_01-05-15.pdf.

Risk management is the ongoing process of identifying, assessing, and responding to risk. To manage risk, organizations should understand the likelihood that an event will occur and the potential resulting impacts. With this information, organizations can determine the acceptable level of risk for achieving their organizational objectives and express this as their risk tolerance.

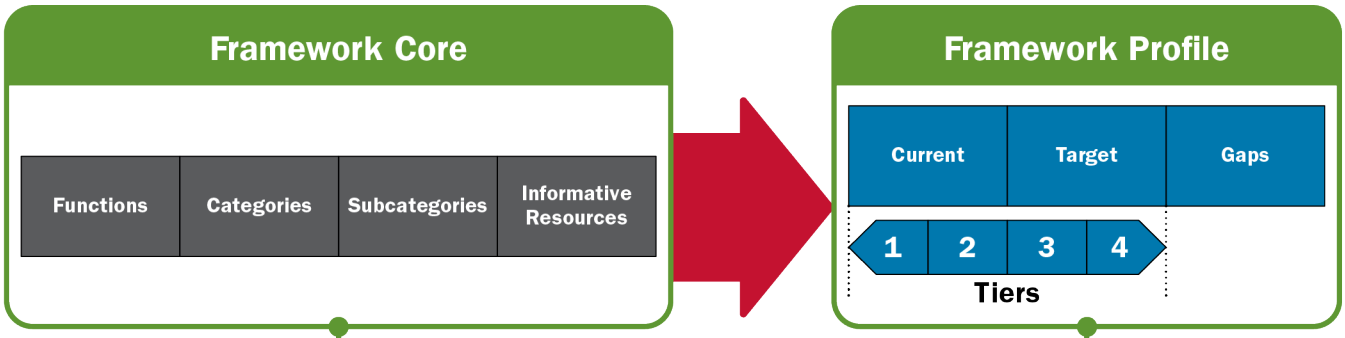
With an understanding of risk tolerance, organizations can prioritize cybersecurity activities, make informed decisions about cybersecurity expenditures, and effectively communicate cybersecurity risk management practices to their partners and service providers. The Framework uses risk management plans (RMPs) to enable organizations to inform and prioritize decisions regarding cybersecurity. It supports recurring risk assessments and validation of business drivers to help organizations select target states for cybersecurity activities that reflect desired outcomes. The Framework gives organizations the ability to dynamically select and direct improvement in cybersecurity risk management for the IT and ICS environments.

The Framework complements, and does not replace, an organization's RMP and cybersecurity program. Alternatively, an organization without an existing cybersecurity program can use the Framework as a reference to establish one.

Framework Structure

The Framework is composed of three parts: the Framework Core, Informative References, and the Framework Profiles.

FIGURE 1. Framework Structure



The **Framework Core** is a set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors. The Core presents industry standards, guidelines, and practices in a manner that allows for communication of cybersecurity activities and outcomes across the organization from the executive level to the implementation/operations level.

The **Framework Core** consists of five concurrent and continuous Functions—Identify, Protect, Detect, Respond, Recover. When considered together, these Functions provide a high-level, strategic view of the lifecycle of an organization's management of cybersecurity risk.

The **Framework Core** then identifies underlying key Categories and Subcategories—which are discrete outcomes for each Function—and matches them with example informative references such as existing standards, guidelines, and practices for each Subcategory.

Informative References are specific sections of standards, guidelines, and practices common among critical infrastructure sectors or specific to a sector that illustrate a method to achieve the outcomes associated with each Subcategory or align their guidance or requirements with the specific Subcategory.

The Informative References presented in the Framework Core are illustrative and not exhaustive. They are based upon cross-sector guidance most frequently referenced during the Framework development process or sector-specific Cybersecurity Tools and Resources identified by sector partners to support framework implementation.

A **Framework Profile** represents the outcomes based on business needs that an organization has selected from the Framework Categories and Subcategories. The Profile can be characterized as the alignment of standards, guidelines, and practices with the Framework Core in a particular implementation scenario.

Profiles can be used to communicate within or between organizations or identify opportunities for improving cybersecurity posture by comparing a "Current" Profile (the "as is" state) with a "Target" Profile (the "to be" state).

To develop a Profile, an organization can review all of the Categories and Subcategories and, based on business/mission drivers and a risk assessment, determine which are most important.

Framework Implementation Tiers provide context on how an organization views cybersecurity risk and the processes in place to manage that risk. Tiers describe the degree to which an organization's cybersecurity risk management practices exhibit the characteristics defined in the Framework (e.g., risk and threat aware, repeatable, and adaptive). The Tiers characterize an organization's practices over a range, from Partial (Tier 1) to Adaptive (Tier 4).

Framework Core

The Framework Core elements work together as follows:

- **Functions** organize basic cybersecurity activities at their highest level. They aid an organization in expressing its management of cybersecurity risk by organizing information, enabling risk management decisions, addressing threats, and improving by learning from previous activities. The Functions also align with existing methodologies for incident management and help show the effect of investments in cybersecurity. For example, investments in planning and exercises support timely response and recovery actions, resulting in reduced impact to the delivery of services. The five Framework Core functions are:
    - **Identify:** Develop an organizational understanding to manage the cybersecurity risks to systems, people, assets, data, and capabilities;
    - **Protect:** Develop and implement appropriate safeguards to ensure delivery of critical services;
    - **Detect:** Develop and implement appropriate activities to identify the occurrence of a cybersecurity event;
    - **Respond:** Develop and implement appropriate activities to take action regarding a detected cybersecurity incident; and
    - **Recover:** Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.
- **Categories** are the subdivisions of a Function into groups of cybersecurity outcomes closely tied to programmatic needs and particular activities. Examples of Categories include "Asset Management," "Identity Management and Access Control," and "Detection Processes." A complete list of Categories can be found in Appendix A, Table Six.
- **Subcategories** further divide a Category into specific outcomes of technical and/or management activities. They provide a set of results that, while not exhaustive, help support achievement of the outcomes in each Category. Examples of Subcategories include "External information systems are catalogued," "Data-at-rest is protected," and "Notifications from detection systems are investigated." A complete list of Subcategories can be found in Appendix A, Table Six.
- **Informative References** are specific sections of standards, guidelines, and practices common among critical infrastructure sectors that illustrate a method to achieve the outcomes associated with each Subcategory. The Informative References presented in the Framework Core are illustrative and not exhaustive. They are based upon cross-sector guidance most frequently referenced during the Framework development process. A complete list of Informative References can be found on the NIST Cybersecurity Framework Informative References page.

TABLE 1. Framework Functions, Categories, Subcategories, and Informative Resources

Table 1 below provides illustrative examples of the subcategories and informative resources. A complete table is available in Appendix A.

Functions	Categories	Subcategories	Informative References
IDENTIFY	Asset Management	Ex: Organizational communication and data flows are mapped	Ex: NIST SP 800-53: AC-4, CA-3, CA-9, PL-8, etc.
		Ex: Resources are prioritized based on their classification, criticality, and business value	Ex: NIST SP 800-53: CP-2, RA-2, SA-14, etc.
	Business Environment		
	Governance		
	Risk Assessment		
	Risk Management Strategy		
	Supply Chain Risk Management		
PROTECT	Identity Management and Access Control		
	Awareness and Training		
	Data Security		
	Information Protection Processes and Procedures		
	Maintenance		

Functions	Categories	Subcategories	Informative References
	Protective Technology		
DETECT	Anomalies and Events		
	Security Continuous Monitoring		
	Detection Processes		
RESPOND	Response Planning		
	Communications		
	Analysis		
	Mitigation		
	Improvements		
RECOVER	Recovery Planning		
	Improvements		
	Communications		

Framework Profile

The Profile is the alignment of the Functions, Categories, and Subcategories with the business requirements, risk tolerance, and resources of the organization. A Profile enables organizations to establish a roadmap for reducing cybersecurity risk that is well-aligned with organizational and sector goals, considers legal/regulatory requirements and industry best practices, and reflects risk management priorities. Given the complexity of many organizations, they may choose to have multiple profiles aligned with particular organizational components to recognize the unique needs of different components.

Framework Profiles can be used to describe the current state or the desired target state of specific cybersecurity activities. The Current Profile indicates the cybersecurity outcomes that are currently being achieved. The Target Profile indicates the outcomes needed to achieve the desired cybersecurity risk management goals. Profiles support business/mission requirements and aid in communicating risk within and between organizations.

Framework Implementation Tiers

The Tiers provide context on how an organization views cybersecurity risk and the processes in place to manage that risk. Ranging from Partial (Tier 1) to Adaptive (Tier 4), Tiers describe an increasing degree of sophistication in cybersecurity risk management practices. They help determine the extent to which cybersecurity risk management is informed by business needs and is integrated into an organization's overall risk management practices.

While organizations identified as Tier 1 are encouraged to consider moving toward Tier 2 or greater, Tiers do not represent maturity levels. Tiers are meant to support organizational decision-making about how to manage cybersecurity risk, as well as which dimensions of the organization are higher priority and could receive additional resources. Progression to higher Tiers is encouraged when a cost-benefit analysis (CBA) indicates a feasible and cost-effective reduction of cybersecurity risk. An organization completes a successful implementation of the Framework when it achieves the outcomes described in its Target Profiles; however, Tier selection and designation naturally affect Framework Profiles.[13]

The Tier definitions are as follows:

Tier 1: Partial

- **Risk Management Process**: Organizational cybersecurity risk management practices are not formalized, and risk is managed in an *ad hoc* and sometimes reactive manner.
- **Integrated Risk Management Program**: There is limited awareness of cybersecurity risk at the organizational level. The organization implements cybersecurity risk management on an irregular, case-by-case basis due to varied experience or information gained from outside sources.
- **External Participation**: The organization does not understand its role in the larger ecosystem of its dependencies or dependents. The organization does not collaborate with or receive information (e.g., threat intelligence, best practices, technologies) from other entities (e.g., buyers, suppliers, dependencies, dependents, Information Sharing and Analysis Organizations, researchers, governments), nor does it share information.

[13] National Institute of Standards and Technology (NIST), *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1, April 16, 2018, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

Tier 2: Risk Informed

- Risk Management Process: Risk management practices are approved by management but may not be established organization-wide.
- Integrated Risk Management Program: There is an awareness of cybersecurity risk at the organizational level, but there is no established organization-wide approach to managing cybersecurity risk. Cybersecurity information is shared within the organization on an informal basis.
- External Participation: Generally, the organization understands its role in the larger ecosystem with respect to either its own dependencies or dependents, but not both. The organization collaborates with and receives some information from other entities and generates some of its own information but may not share information with others.

Tier 3: Repeatable

- Risk Management Process: The organization's risk management practices are formally approved and expressed as policy.
- Integrated Risk Management Program: There is an organization-wide approach to manage cybersecurity risk. Risk-informed policies, processes, and procedures are defined, implemented as intended, and reviewed.
- External Participation: The organization understands its role, dependencies, and dependents in the larger ecosystem and may contribute to the community's broader understanding of risks. It collaborates with and regularly receives information from other entities that complements internally generated information, and shares information with other entities.

Tier 4: Adaptive

- Management Process: The organization adapts its cybersecurity practices based on previous and current cybersecurity activities, including lessons learned and predictive indicators.
- Integrated Risk Management Program: There is an organization-wide approach to managing cybersecurity risk that uses risk-informed policies, processes, and procedures to address potential cybersecurity events. The relationship between cybersecurity risk and organizational objectives is clearly understood and considered when making decisions.
- External Participation: The organization understands its role, dependencies, and dependents in the larger ecosystem and contributes to the community's broader understanding of risks. It receives, generates, and reviews prioritized information that informs continuous analysis of its risks as the threat and technology landscapes evolve. The organization shares that information internally and externally with other collaborators.

Framework Implementation

The Framework illustrates the informational and decision flows within an organization. For example, senior executives gauge priorities for business levels to nominate Tiers to develop profiles, which then go to the operational level of an organization that implements the profile. An organization can use the Framework as a key part of its systematic process for identifying, assessing, and managing cybersecurity risk. The Framework is not designed to replace existing processes; rather, it is designed to complement existing business and cybersecurity operations. It can serve as the foundation for a new cybersecurity program or a mechanism for improving an existing program. It also provides a general set of considerations and processes for considering privacy and civil liberties implications in the context of a cybersecurity program.

Considerations Prior to Implementation

There are some considerations that can be considered prior to implementation. They are as follows:

- **Communicating Cybersecurity Requirements with Stakeholders**: The Framework provides a common language to communicate requirements among interdependent stakeholders responsible for the delivery of essential critical infrastructure products and services. Communication is especially important among stakeholders up and down supply chains. Supply chains begin with the sourcing of products and services and extend from the design, development, manufacturing, processing, handling, and delivery of products and services to the end user. Given these complex and interconnected relationships, supply chain risk management (SCRM) is a critical organizational function.[14]
    - Cyber SCRM is the set of activities necessary to manage cybersecurity risk associated with external parties. A primary objective of cyber SCRM is to identify, assess, and mitigate cyber supply chain risks associated with "products and services that may contain potentially malicious functionality, are counterfeit, or are vulnerable due to poor manufacturing and development practices" within the cyber supply chain.[15]
- **Buying Decisions**: Since a Framework Target Profile is a prioritized list of organizational cybersecurity requirements, Target Profiles can be used to inform decisions about buying products and services. This transaction varies from Communicating Cybersecurity Requirements with Stakeholders in that it may not be possible to impose a set of cybersecurity requirements on the supplier. The objective should be to make the best buying decision among multiple suppliers, given a carefully determined list of cybersecurity requirements. Once a product or service is purchased, the Profile also can be used to track and address residual cybersecurity risk.
- **Identifying Opportunities for New or Revised Informative References**: The Framework can be used to identify opportunities for new or revised standards, guidelines, or practices where additional Informative References would help organizations address emerging needs. An organization

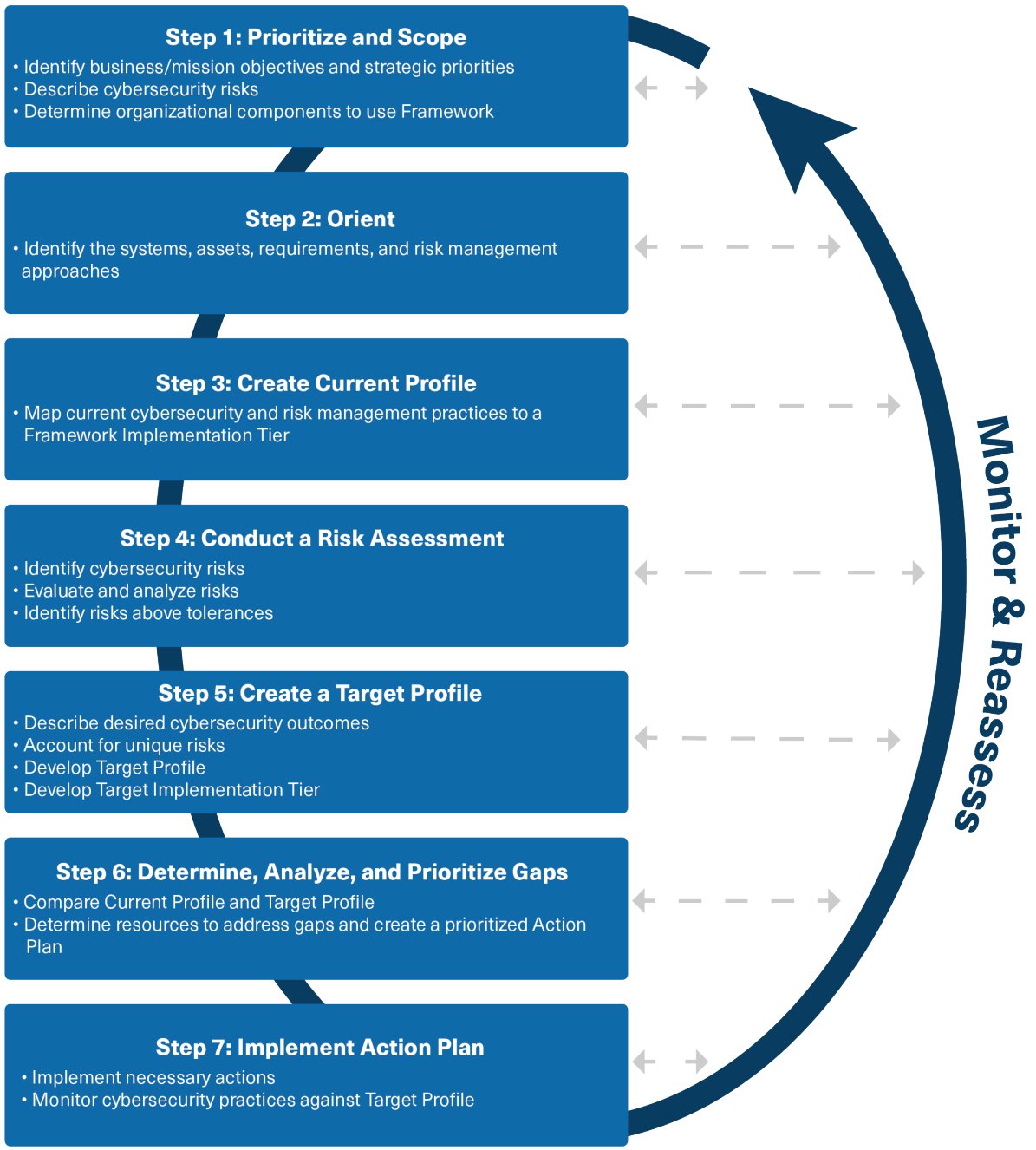
[14] Communicating Cybersecurity Requirements (Section 3.3) and Buying Decisions (Section 3.4) address only two uses of the Framework for cyber SCRM and are not intended to address cyber SCRM comprehensively.
[15] NIST Special Publication 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, Boyens et al, April 2015, https://doi.org/10.6028/NIST.SP.800-161.

implementing a given Subcategory, or developing a new Subcategory, might discover that there are few Informative References, if any, for a related activity.

Step-by-Step Framework Implementation Guide

The Framework can be applied through a seven-step process, shown below in Figure 2.

FIGURE 2. Seven-step Process for Framework Implementation



Implementation should include a plan to communicate progress to appropriate stakeholders, such as senior management. This process should integrate into an organization's risk management program and provide feedback and validation to previous steps. Validation and feedback provide a mechanism for process improvement and can increase the overall effectiveness and efficiency of the process.

Step 1: Prioritize and Scope

When implementing the Framework, an organization first identifies its business or mission objectives and its strategic priorities as they relate to cybersecurity. With this information, an organization can make decisions regarding cybersecurity implementation and determine the breadth and scope of systems and assets that support its objectives. An organization can adapt the Framework to support different business lines or processes, which may have different business needs and associated risk tolerance.

Typical risk management processes include a strategy that frames, assesses, responds to, and monitors risk. Larger enterprises may already use a strategic-level approach to which the enterprise's organizations subscribe. Whether an organization uses a unique approach or that of a larger enterprise, an applicable strategy should describe the identified cybersecurity risks that the organization considers when making investment and operational decisions.

Current threat and vulnerability information (e.g., information from important vendors, communication of Commercial Facilities Sector threats from an information sharing and analysis center, or other threat advisories) may also help inform scoping decisions.

In order to gain familiarity and experience, an organization using the Framework for the first time may apply it to a small subset of operations. For example, an organization may choose to begin with particular business functions because they are already undergoing similar or related risk management efforts. Then, with a greater understanding, the organization can apply the Framework to a broader subset of operations or to additional divisions of the organization.

Step 2: Orient

At this stage, an organization identifies the systems, assets, requirements, and risk management approaches that fall within the scope of the effort. This includes current organization standards and best practices, as well as any additional items that can enable the organization to achieve its critical infrastructure and business objectives for cybersecurity risk management. The organization's risk management program may have already identified and documented much of this information. In general, organizations should focus initially on critical systems and assets and then expand into systems and assets that are less critical or central to their mission.

Additionally, an organization should identify the approach to determine its current risk management and cybersecurity posture. Organizations can use a variety of methods to identify their current cybersecurity posture and create a Current Profile, including self-evaluations or facilitated approaches. In a self-evaluation, an organization may leverage its own resources and expertise, whereas a facilitated approach relies on the expertise of a third party. The value in a self-evaluation is the additional internal cybersecurity awareness and discovery that the activity can generate.

Step 3: Create a Current Profile

The organization develops a Current Profile by indicating which Category and Subcategory outcomes from the Framework Core are currently being achieved. The purpose of identifying a Current Profile is not only to develop a map between organizational practices and Category and Subcategory outcomes, but also to help understand the extent to which such practices achieve the outcomes outlined by the Framework. To identify

the Current Profile, organizations use the evaluation approach (e.g., self-evaluation or facilitated approach) identified in Step 2 to map current cybersecurity approach and outcomes to the corresponding Category and Subcategory outcomes. In many cases, organizations may be able to leverage existing efforts to facilitate this activity. For example, as a part of their risk assessment programs, organizations may have addressed their current state through regular evaluations or internal audits.

The current Implementation Tier describes the degree of rigor and sophistication of the in-scope cybersecurity risk management program (i.e., the Framework usage scope defined in Step 1). To identify the Implementation Tier, the organization maps its current approach to the Implementation Tier descriptions in the Framework document. Implementation Tiers do not apply to the individual Category and Subcategory outcomes in the Framework Core; the organization identifies an Implementation Tier for the in-scope cybersecurity and risk management program as a whole.

Organizations may already be using tools, standards, and processes or complying with industry standards that closely align with the Framework. Some industry and standards organizations have started to publish their own guidance to map existing standards and tools to the Framework elements to facilitate implementation.

Table 2 provides an example of how a mapping can be used to create a Current Profile for a specific Subcategory outcome (see Section PR.AC-3 of the Framework document) for three organizations using three different approaches. A similar table could be built for Implementation Tiers, keeping in mind that Tiers are focused at broader program level risk management. Note that the examples in these tables are intended to be illustrative of the mapping concept and are unlikely to address any specific organization's particular approach. The level of specificity and granularity required for a Profile to be useful will be unique to each organization.

The three organizations in Table 2 each take different approaches to managing remote access control to their services.

TABLE 2. Connecting Organizational Approach to Framework

Organization 1 Internal Controls Approach			
Function	Category	Subcategory	Profile Current
PROTECT (PR)	Access Control (PR.AC)	PR.AC-3: Remote access is managed	• Dial-in access for vendor maintenance is enabled as required and disabled when maintenance window completes • Remote access only authorized via encrypted VPN service • Remote access activity logged and monitored • Access to VPN service restricted to organization-approved devices • All unauthorized connection attempts to VPN are logged • Immediate disabling of VPN account upon employee termination
Organization 2 Standards Based Approach			
Function	Category	Subcategory	Profile Current

PROTECT (PR)	Access Control (PR.AC)	PR.AC-3: Remote access is managed	• NIST SP 800-53 Rev 4 AC-17 • NIST SP 800-53 Rev 4 AC-17 (1) • NIST SP 800-53 Rev 4 AC-17 (2) • NIST SP 800-53 Rev 4 AC-19 • NIST SP 800-53 Rev 4 AC-20 • NIST SP 800-53 Rev 4 AC-20 (1)
Organization 3 Exception Approach			
Function	Category	Subcategory	Profile
			Current
PROTECT (PR)	Access Control (PR.AC)	PR.AC-3: Remote access is managed	• Not Applicable—No remote access available for in-scope assets and systems

Even though the Framework gives organizations a broad overview of the cybersecurity and risk management domains, it is not all-inclusive, and the organization may have already utilized standards, tools, methods, and guidelines that achieve outcomes not defined by or referenced in the Framework. The Current Profile should identify these practices as well. When appropriate, organizations should consider sharing these practices with NIST to help strengthen and expand the Framework.

Step 4: Conduct a Risk Assessment

This assessment could be guided by the organization's overall risk management process or previous risk assessment activities. The organization analyzes the operational environment in order to discern the likelihood of a cybersecurity event and the impact that the event could have on the organization. It is important that the organization incorporates emerging risk, threat, and vulnerability data to facilitate a robust understanding of the likelihood and impact of cybersecurity events. The results of cybersecurity risk assessment activities allow the organization to develop its Target Profile and identify a Target Implementation Tier, which occurs in Step 5. For organizations that already have a risk management program in place, this activity will be part of regular business practice, and necessary records and information to make this determination may already exist.

Step 5: Create a Target Profile

In creating a Target Profile, organizations should consider:

- current risk management practices,
- current risk environment,
- legal and regulatory requirements,
- business and mission objectives, and
- organizational constraints.

The Target Profile outlines the key Category and Subcategory outcomes and associated cybersecurity and risk management standards, tools, methods, and guidelines that will protect against cybersecurity risks in proportion to the risks facing organizational and critical infrastructure security objectives. As highlighted in Step 3, the Framework gives organizations a broad overview of the cybersecurity and risk management domains, but it is not all-inclusive. An organization may find it necessary to use standards, tools, methods,

and guidelines that achieve outcomes not defined by the Framework. Including these practices in the Target Profile is also beneficial for coordination and future engagement.

Table 3 gives an overview of a hypothetical Target Profile for a specific Subcategory outcome (PR.AC-3) for three organizations using three different approaches. The bold text in the Target Profile highlights where the organization has identified additional practices it desires to use in order to successfully achieve an outcome based on its current risk environment and business and critical infrastructure objectives. Organization 1 has determined that the existing practices it uses for managing remote access are insufficient for addressing its unique risk environment and that additional practices are required. Organization 2 arrives at the same conclusion and identifies additional standards it would like to deploy across the in-scope organization. Organization 3 demonstrates an organization whose Current Profile is identical to the Target Profile for this Subcategory outcome. Such instances will occur when the standards, tools, methods, and guidelines currently deployed by the organization sufficiently fulfill its cybersecurity and risk management requirements. However, this alignment of the Current Profile and Target Profile may only last over the short term since an organization's cybersecurity and risk management requirements will evolve as its risk and operational environments change over time. For instance, an organization may determine that a current practice is no longer necessary or is inadequate and, therefore, omit it from the Target Profile.

In developing a Target Profile, organizations may opt to use a broad approach—considering more effective and efficient risk management approaches across the entire in-scope organizations—rather than examining individual Categories and Subcategories.

In addition to the Target Profile, the organization selects a Target Implementation Tier that applies to the in-scope risk management process. The organization examines each Tier and selects its target (the "desired" state) using the same list of considerations above for the Target Profile. Once a Target Implementation Tier is selected, the organization identifies the cybersecurity practices and risk management activities necessary to achieve that target—considering their ability to meet organizational goals, feasibility to implement, and their ability to reduce cybersecurity risks to acceptable levels for critical assets and resources (i.e., those most important to achieving the organization's business and critical infrastructure objectives).

Using its collection of cybersecurity and risk management standards, tools, methods, and guidelines, the organization documents these desired outcomes in the Target Profile and Target Implementation Tier.

TABLE 3. Creating a Target Profile

Organization 1 Internal Controls Approach				
Function	Category	Subcategory	Profile	
			Current	Target
PROTECT (PR)	Access Control (PR.AC)	PR.AC-3: Remote access is managed	• Dial-in access for vendor maintenance is enabled as required and disabled when maintenance window completes • Remote access only authorized via encrypted VPN service • Remote access activity logged and monitored • Access to VPN service restricted to organization-approved devices • All unauthorized connection attempts to VPN are logged • Immediate disabling of VPN account upon employee termination	• Dial-in access for vendor maintenance is enabled as required and disabled when maintenance window completes • Remote access only authorized via encrypted VPN service • Remote access activity logged and monitored • Access to VPN service restricted to organization-approved devices • All unauthorized connection attempts to VPN are logged • Immediate disabling of VPN account upon employee termination • **Supervisor signature required before VPN account issued** • **Biannual review of authorized VPN account list**
Organization 2 Standards Based Approach				
Function	Category	Subcategory	Profile	
			Current	Target
PROTECT (PR)	Access Control (PR.AC)	PR.AC-3: Remote access is managed	• NIST SP 800-53 Rev 4 AC-17 • NIST SP 800-53 Rev 4 AC-17 (1) • NIST SP 800-53 Rev 4 AC-17 (2) • NIST SP 800-53 Rev 4 AC-19 • NIST SP 800-53 Rev 4 AC-20 • NIST SP 800-53 Rev 4 AC-20 (1)	• NIST SP 800-53 Rev 4 AC-17 • NIST SP 800-53 Rev 4 AC-17 (1) • NIST SP 800-53 Rev 4 AC-17 (2) • **NIST SP 800-53 Rev 4 AC-17 (3)** • **NIST SP 800-53 Rev 4 AC-17 (4)** • NIST SP 800-53 Rev 4 AC-19 • **NIST SP 800-53 Rev 4 AC-19 (5)** • NIST SP 800-53 Rev 4 AC-20 • NIST SP 800-53 Rev 4 AC-20 (1) • **NIST SP 800-53 Rev 4 AC-20 (2)**
Organization 3 Exception Approach				
Function	Category	Subcategory	Profile	
			Current	Target
PROTECT (PR)	Access Control (PR.AC)	PR.AC-3: Remote access is managed	• Not Applicable—No remote access available for in-scope assets and systems	• Not applicable—No remote access available for in-scope assets and systems

Bold text highlights the differences between the current and target approaches.

Step 6: Determine, Analyze, and Prioritize Gaps

The organization compares the Current Profile and the Target Profile to determine gaps. To address those gaps, it creates a prioritized action plan that draws on mission drivers, a cost/benefit analysis, and an understanding of risk to achieve the outcomes in the Target Profile. The organization then determines resources necessary to address the gaps. Using Profiles in this manner enables the organization to make informed decisions about cybersecurity activities, supports risk management, and allows the organization to perform cost-effective, targeted improvements. Table 4 provides an overview of a hypothetical gap analysis for a specific Subcategory outcome (PR.AC-3) for three organizations using three different approaches.

A gap exists when there is a desired Category or Subcategory outcome in the Target Profile or program characteristic in the Target Implementation Tier that is not currently satisfied by current cybersecurity and risk management approaches, as well as situations wherein existing practices do not achieve the outcome to the degree of satisfaction required by the organization's risk management strategy. After identifying gaps in both the Profile and Tier, the organization identifies the potential consequences of failing to address such issues. At this point, the organization should assign a mitigation priority to all identified gaps. Prioritization of gaps should include examination of existing risk management practices, the current risk environment, legal and regulatory requirements, business and mission objectives, and any other applicable organizational limitations or considerations.

Once each gap is assigned a mitigation priority, the organization determines potential mitigation efforts and performs a CBA on each option. The organization creates a plan of prioritized mitigation actions—based on available resources, business needs, and current risk environment—to move from the existing state to the desired or target state. If the organization is at its target state, it would seek to maintain its security posture in the face of ongoing changes to the risk environment.

TABLE 4. Identifying Implementation Gaps

Organization 1 Internal Controls Approach					
Function	Category	Subcategory	Profile		
			Current	Target	Gaps
PROTECT (PR)	Access Control (PR.AC)	PR.AC-3: Remote access is managed	• Dial-in access for vendor maintenance is enabled as required and disabled when maintenance window completes • Remote access only authorized via encrypted VPN service • Remote access activity logged and monitored • Access to VPN service restricted to organization-approved devices • All unauthorized connection attempts to VPN are logged • Immediate disabling of VPN account upon employee termination	• Dial-in access for vendor maintenance is enabled as required and disabled when maintenance window completes • Remote access only authorized via encrypted VPN service • Remote access activity logged and monitored • Access to VPN service restricted to organization-approved devices • All unauthorized connection attempts to VPN are logged • Immediate disabling of VPN account upon employee termination • Supervisor signature required before VPN account issued • Biannual review of authorized VPN account list	• Supervisor signature required before VPN account issued • Biannual review of authorized VPN account list

Organization 2 Standards Based Approach					
Function	Category	Subcategory	Profile		
			Current	Target	Gaps
PROTECT (PR)	Access Control (PR.AC)	PR.AC-3: Remote access is managed	• NIST SP 800-53 Rev 4 AC-17 • NIST SP 800-53 Rev 4 AC-17 (1) • NIST SP 800-53 Rev 4 AC-17 (2) • NIST SP 800-53 Rev 4 AC-19 • NIST SP 800-53 Rev 4 AC-20 • NIST SP 800-53 Rev 4 AC-20 (1)	• NIST SP 800-53 Rev 4 AC-17 • NIST SP 800-53 Rev 4 AC-17 (1) • NIST SP 800-53 Rev 4 AC-17 (2) • NIST SP 800-53 Rev 4 AC-17 (3) • NIST SP 800-53 Rev 4 AC-17 (4) • NIST SP 800-53 Rev 4 AC-19 • NIST SP 800-53 Rev 4 AC-19 (5) • NIST SP 800-53 Rev 4 AC-20 • NIST SP 800-53 Rev 4 AC-20 (1) • NIST SP 800-53 Rev 4 AC-20 (2)	• NIST SP 800-53 Rev 4 AC-17 (3) • NIST SP 800-53 Rev 4 AC-17 (4) • NIST SP 800-53 Rev 4 AC-19 (5) • NIST SP 800-53 Rev 4 AC-20 (2)

Organization 3 Exception Approach					
Function	Category	Subcategory	Profile		
			Current	Target	Gaps
PROTECT (PR)	Access Control (PR.AC)	PR.AC-3: Remote access is managed	• Not Applicable—No remote access available for in-scope assets and systems	• Not Applicable—No remote access available for in-scope assets and systems	• None

Step 7: Implement Action Plan

The organization determines which actions to take regarding the gaps (if any) identified in the previous step, and then monitors its current cybersecurity practices against the Target Profile. For further guidance, the Framework identifies Informative References regarding the Categories and Subcategories. Organizations should determine which standards, guidelines, and practices, including those that are sector-specific, work best for their needs.

An organization may repeat the steps as needed to continuously assess and improve its cybersecurity. For instance, organizations may find that more frequent repetition of the orient step improves the quality of risk assessments. Furthermore, organizations may monitor progress through iterative updates to the Current Profile, subsequently comparing the Current Profile to the Target Profile. Organizations may also utilize this process to align their cybersecurity program with their desired Framework Implementation Tier.

Conclusion

This document serves as a foundation for how Commercial Facilities Sector organizations can leverage existing resources to increase their overall cybersecurity awareness using the NIST Framework for Improving Critical Infrastructure Cybersecurity. Specifically, the information provided in this document can aid an organization to assess its current cybersecurity practices, identify tools that assist in revealing gaps, and determine its cybersecurity goals. For additional information, please visit www.cisa.gov.

Appendix A: Cybersecurity Tools and Resources to Support Framework Implementation

The Framework's Informative References[16] mapped a set of broad national and international cybersecurity standards to the Framework Core, providing owners and operators with sample methods to achieve the cybersecurity outcomes described by each Function, Category, and Subcategory. The six Informative References are listed below. They apply broadly across critical infrastructure sectors and could be considered in implementing specific controls.[17]

The cybersecurity tools and resources listed in this document are for informational and educational purposes only. CISA does not guarantee their content or endorse any specific person, entity, product, service, or enterprise. The tools and resources identified in this document do not encompass all tools and resources available to owners and operators. Access to some of those tools and resources may require a fee, paid subscription, and/or organizational membership; the use or adoption of such paid tools or resources is entirely at the discretion of each organization.

- American National Standards Institute/International Society of Automation (ANSI/ISA)-62443-2-1 (99.02.01)-2009, Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program: This standard is applicable for identifying elements in cybersecurity management systems for industrial automation and control systems.
- ANSI/ISA-62443-3-3 (99.03.03)-2013, Security for Industrial Automation and Control Systems: System Security Requirements and Security Levels: This standard provides detailed technical control system requirements and the requirements for control system capability security levels.
- CIS Critical Security Controls for Effective Cyber Defense (CIS Controls): The CIS Security Controls include 20 courses of action, as well as other resources for cyber defense.
- Control Objectives for Information and Related Technology (COBIT): This framework provides a platform for strategic governance of enterprise information and technology, combining IT governance with business risk management.
- ISO/IEC 27001, Information technology—Security techniques—Information security management systems—Requirements: This standard outlines the requirements for establishing, implementing, maintaining, and continually improving an information security management system for all types of organizations.
- NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations: This publication provides a catalog of security and privacy controls for Federal information systems and organizations and a process for selecting controls.

This section outlines additional existing cybersecurity tools, standards, and approaches used within the Commercial Facilities Sector and provides an initial mapping of those methods to the Functions, Categories, and Subcategories.

[16] References are specific sections of standards, guidelines, and practices. The Framework identified several national and international standards that organizations can use to achieve the outcomes in each Subcategory. See Framework Core for more information.

[17] The CIS Security Controls for Effective Cyber Defense and NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations are available online for free.

This mapping may help Commercial Facilities Sector owners and operators identify additional tools and resources—many of which they may already be using or considering—that can help them implement the Framework or demonstrate how they are already applying Framework concepts. Table 5a includes directly applicable resources, while Table 5b offers supplemental guidance.

TABLE 5a. Commercial Facilities Sector Cybersecurity Risk Management Direct Guidance

Name	Summary	Additional Information
Direct Resources		
Payment Card Industry Data Security Standards (PCI-DSS)	PCI-DSS establishes worldwide information security standards to help organizations that process card payments prevent credit card fraud through increased controls around data and its exposure to compromise. The standard applies to all organizations that hold, process, or pass cardholder information from any card branded with the logo of one of the card brands.	Payment Card Industry Data Security Standards
Stadium Cybersecurity Best Practices Guide	This guide recommends cybersecurity best practices by examining control systems, enterprise systems, and communication systems that stadiums and arenas typically rely on for essential operations. It also provides a first estimate of the risk level associated with each asset.	Stadium Cybersecurity Best Practices Guide (For Official Use Only [FOUO]; available on Homeland Security Information Network – Critical Infrastructure [HSIN-CI])
Cyber Resilience Review (CRR)	The CRR assesses enterprise programs and practices across a range of 10 domains, including risk management, incident management, service continuity, and others. The assessment is designed to measure existing organizational resilience, as well as to provide a gap analysis for improvement based on recognized best practices.	CRR Information CRR NIST Framework Crosswalk
Cybersecurity Evaluation Tool (CSET)	The CSET guides users through a step-by-step process to assess their control system and information technology network security practices against recognized industry standards.	CSET Fact Sheet
Baldrige Cybersecurity Excellence Builder (BCEB), Version 1.1	The BCEB provides a self-assessment tool to help organizations better understand the effectiveness of their cybersecurity risk management efforts and identify improvement opportunities in the context of their overall organizational performance. The self-assessment tool blends organizational assessment approaches from the Baldrige Performance Excellence Program with the concepts and principles of the NIST Cybersecurity Framework.	Baldrige Cybersecurity Excellence Builder

Table 5b. Commercial Facilities Sector Cybersecurity Risk Management Supplemental Guidance

Supplemental Resources		
Federal Virtual Training Environment (FedVTE)	FedVTE provides online cybersecurity training for Federal, State, local, tribal, or territorial government personnel and veterans. Managed by DHS, FedVTE contains more than 800 hours of training on topics including ethical hacking and surveillance, risk management, and malware analysis.	FedVTE Cybersecurity Training
National Cybersecurity Workforce Framework	The National Cybersecurity Workforce Framework categorizes and provides a common language to describe cybersecurity work. It lists tasks and requisite knowledge, skills, and abilities for over 30 specialty areas.	National Security Workforce Framework
Cybersecurity Training Catalog	The Cybersecurity Training Catalog provides information that enables the Nation to access thousands of cybersecurity courses from providers across the Nation. It can help sector organizations close skill gaps in the cyber workforce.	Cybersecurity Training Catalog

Subject matter experts identified existing cybersecurity tools and approaches in the Commercial Facilities Sector and evaluated them against the Functions, Categories, and Subcategories of the Framework. When all or a portion of an existing tool or approach was determined to align with a particular Subcategory, it was marked as such in Table 6. To determine whether a tool or approach maps to a particular Subcategory, the sector considered a key question: can the tool or approach help an organization further understand or address the particular Subcategory and achieve the associated outcome? Based on this question, many sector-level documents and approaches do help organizations address the Framework.

The initial mapping is a first attempt at aligning existing tools and approaches with the Framework using open-source research. In some cases, access to the tools and approaches was not available via open-source research, so fact sheets and program descriptions were used to hypothesize where tools and approaches aligned. This mapping is designed to be altered in future versions by sector stakeholders with a solid understanding of the tools and approaches.

TABLE 6. Commercial Facilities Sector Framework Mapping Matrix

Function	Category	Subcategory	PCI-DSS	CRR	CSET	BCEB	Stadium Guide	ISO 27001/2	COBIT	CSC
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	**ID.AM-1**: Physical devices and systems within the organization are inventoried	X	X	X	X	X	X	X	X
		ID.AM-2: Software platforms and applications within the organization are inventoried	X	X	X	X	X	X	X	X
		ID.AM-3: Organizational communication and data flows are mapped	X	X	X	X	X	X	X	X
		ID.AM-4: External information systems are catalogued	X	X	X	X		X	X	
		ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	X	X	X	X	X	X	X	
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	X	X	X	X	X	X	X	
IDENTIFY (ID)	**Business Environment (ID.BE):** The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform	**ID.BE-1:** The organization's role in the supply chain is identified and communicated		X	X	X		X	X	
		ID.BE-2: The organization's place in critical infrastructure and its industry		X	X	X		X	X	

Function	Category	Subcategory	PCI-DSS	CRR	CSET	BCEB	Stadium Guide	ISO 27001/2	COBIT	CSC
	cybersecurity roles, responsibilities, and risk management decisions.	sector is identified and communicated								
		ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated		X	X	X			X	
		ID.BE-4: Dependencies and critical functions for delivery of critical services are established		X	X	X	X	X		
		ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g., under duress/attack, during recovery, normal operations)	X	X	X	X		X	X	

Function	Category	Subcategory	PCI-DSS	CRR	CSET	BCEB	Stadium Guide	ISO 27001/2	COBIT	CSC
IDENTIFY (ID)	**Governance (ID.GV):** The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	**ID.GV-1:** Organizational cybersecurity policy is established and communicated	X	X	X	X		X	X	
		ID.GV-2: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners	X	X	X	X	X	X	X	
		ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	X	X	X	X		X	X	
		ID.GV-4: Governance and risk management processes address cybersecurity risks	X	X	X	X	X		X	
IDENTIFY (ID)	**Risk Assessment (ID.RA):** The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**ID.RA-1:** Asset vulnerabilities are identified and documented	X	X	X	X	X	X	X	X
		ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources	X	X	X	X		X		
		ID.RA-3: Threats, both internal and external, are identified and documented	X	X	X	X			X	
		ID.RA-4: Potential business impacts and likelihoods are identified	X	X	X	X	X		X	
		ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	X	X	X	X		X	X	
		ID.RA-6: Risk responses are identified and prioritized	X	X	X	X			X	
IDENTIFY (ID)	**Risk Management Strategy (ID.RM):** The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	**ID.RM-1:** Risk management processes are established, managed, and agreed to by organizational stakeholders	X	X	X	X			X	
		ID.RM-2: Organizational risk tolerance is determined and clearly expressed	X	X	X	X			X	

Function	Category	Subcategory	PCI-DSS	CRR	CSET	BCEB	Stadium Guide	ISO 27001/2	COBIT	CSC
		ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector-specific risk analysis	X	X	X	X				
IDENTIFY (ID)	**Supply Chain Risk Management (ID.SC):** The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	**ID.SC-1:** Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	X		X	X		X	X	X
		ID.SC-2: Suppliers and third-party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process	X		X	X		X	X	
		ID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan	X		X			X	X	
		ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations	X		X	X		X		X
		ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers			X	X		X		

Function	Category	Subcategory	PCI-DSS	CRR	CSET	BCEB	Stadium Guide	ISO 27001/2	COBIT	CSC
PROTECT (PR)	**Identity Management, Authentication and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, or devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	**PR.AC-1:** Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes	X	X	X	X	X	X	X	X
		PR.AC-2: Physical access to assets is managed and protected	X	X	X	X	X	X	X	X
		PR.AC-3: Remote access is managed	X	X	X	X	X	X	X	X
		PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	X	X	X	X	X	X	X	X
		PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)	X	X	X	X	X	X	X	X
		PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions	X	X	X	X	X	X	X	X
		PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	X				X	X	X	X
PROTECT (PR)	**Awareness and Training (PR.AT):** The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.	**PR.AT-1:** All users are informed and trained	X	X	X	X	X	X	X	
		PR.AT-2: Privileged users understand their roles and responsibilities	X	X	X	X	X	X	X	
		PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles and responsibilities	X	X	X	X	X	X	X	X
		PR.AT-4: Senior executives understand their roles and responsibilities	X	X	X	X	X	X		
		PR.AT-5: Physical and cybersecurity personnel understand their roles and responsibilities	X	X	X	X	X	X	X	
PROTECT (PR)	**Data Security (PR.DS):** Information and records (data) are managed	**PR.DS-1:** Data-at-rest is protected	X	X	X	X	X	X	X	X
		PR.DS-2: Data-in-transit is protected	X	X	X	X	X	X	X	

Function	Category	Subcategory	PCI-DSS	CRR	CSET	BCEB	Stadium Guide	ISO 27001/2	COBIT	CSC
	consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**PR.DS-3:** Assets are formally managed throughout removal, transfers, and disposition	X	X	X	X	X	X	X	
		PR.DS-4: Adequate capacity to ensure availability is maintained	X	X	X	X	X	X	X	
		PR.DS-5: Protections against data leaks are implemented	X	X	X	X	X	X	X	
		PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	X	X	X	X	X	X	X	
		PR.DS-7: The development and testing environment(s) are separate from the production environment	X	X	X	X	X		X	
		PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity		X	X	X	X	X		

Function	Category	Subcategory	PCI-DSS	CRR	CSET	BCEB	Stadium Guide	ISO 27001/2	COBIT	CSC
PROTECT (PR)	**Information Protection Processes and Procedures (PR.IP):** Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	**PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g., concept of least functionality)	X	X	X	X	X	X	X	
		PR.IP-2: A System Development Life Cycle to manage systems is implemented	X	X	X	X	X	X	X	
		PR.IP-3: Configuration change control processes are in place	X	X	X	X	X	X	X	
		PR.IP-4: Backups of information are conducted, maintained, and tested	X	X	X	X	X	X		
		PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	X	X	X	X	X	X	X	
		PR.IP-6: Data is destroyed according to policy	X	X	X	X	X	X	X	
		PR.IP-7: Protection processes are improved	X	X	X	X	X	X	X	X
		PR.IP-8: Effectiveness of protection technologies is shared	X	X	X	X	X	X	X	
		PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	X	X	X	X	X	X	X	
		PR.IP-10: Response and recovery plans are tested	X	X	X	X	X	X	X	X
		PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	X	X	X	X	X		X	
		PR.IP-12: A vulnerability management plan is developed and implemented	X	X	X	X	X	X		
PROTECT (PR)	**Maintenance (PR.MA):** Maintenance and repairs of	**PR.MA-1:** Maintenance and repair of organizational assets are performed	X	X	X	X	X			

Function	Category	Subcategory	PCI-DSS	CRR	CSET	BCEB	Stadium Guide	ISO 27001/2	COBIT	CSC
	industrial control and information system components are performed consistent with policies and procedures.	and logged, with approved and controlled tools								
		PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	X	X	X	X	X		X	

Function	Category	Subcategory	PCI-DSS	CRR	CSET	BCEB	Stadium Guide	ISO 27001/2	COBIT	CSC
PROTECT (PR)	**Protective Technology (PR.PT):** Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	**PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	X	X	X		X		X	
		PR.PT-2: Removable media is protected, and its use restricted according to policy	X	X	X		X		X	X
		PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities	X	X	X		X			
		PR.PT-4: Communications and control networks are protected	X	X	X	X	X	X		

Function	Category	Subcategory	PCI-DSS	CRR	CSET	BCEB	Stadium Guide	ISO 27001/2	COBIT	CSC
		PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations		X	X	X	X	X	X	X
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected, and the potential impact of events is understood.	**DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed	X	X	X	X	X	X		
		DE.AE-2: Detected events are analyzed to understand attack targets and methods	X	X	X	X		X	X	
		DE.AE-3: Event data are collected and correlated from multiple sources and sensors	X	X	X	X	X			
		DE.AE-4: Impact of events is determined	X	X	X	X		X	X	
		DE.AE-5: Incident alert thresholds are established	X	X	X	X		X	X	X
DETECT (DE)	**Security Continuous Monitoring (DE.CM):** The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	**DE.CM-1:** The network is monitored to detect potential cybersecurity events	X	X	X	X	X	X		
		DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	X	X	X	X	X	X	X	
		DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	X	X	X	X		X	X	
		DE.CM-4: Malicious code is detected	X	X	X	X	X	X	X	
		DE.CM-5: Unauthorized mobile code is detected	X	X	X	X		X	X	X
		DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	X	X	X	X		X		
		DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	X	X	X	X	X	X		

Function	Category	Subcategory	PCI-DSS	CRR	CSET	BCEB	Stadium Guide	ISO 27001/2	COBIT	CSC
		DE.CM-8: Vulnerability scans are performed	X	X	X	X		X		

Function	Category	Subcategory	PCI-DSS	CRR	CSET	BCEB	Stadium Guide	ISO 27001/2	COBIT	CSC
DETECT (DE)	**Detection Processes (DE.DP):** Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	**DE.DP-1:** Roles and responsibilities for detection are well defined to ensure accountability	X	X	X	X				
		DE.DP-2: Detection activities comply with all applicable requirements	X	X	X	X				
		DE.DP-3: Detection processes are tested	X	X	X	X		X	X	
		DE.DP-4: Event detection information is communicated	X	X	X	X		X		
		DE.DP-5: Detection processes are continuously improved	X	X	X	X		X		
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained to ensure response to detected cybersecurity events.	**RS.RP-1:** Response plan is executed during or after an incident	X	X	X	X		X		
RESPOND (RS)	**Communications (RS.CO):** Response activities are coordinated with internal and external stakeholders (e.g., external support from law enforcement agencies).	**RS.CO-1:** Personnel know their roles and order of operations when a response is needed	X	X	X			X		
		RS.CO-2: Incidents are reported consistent with established criteria	X	X	X			X		
		RS.CO-3: Information is shared consistent with response plans	X	X	X	X		X		
		RS.CO-4: Coordination with stakeholders occurs consistent with response plans	X	X	X	X		X	X	
		RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness		X	X	X				
RESPOND (RS)	**Analysis (RS.AN):** Analysis is conducted to ensure effective response and support recovery activities.	**RS.AN-1:** Notifications from detection systems are investigated	X	X	X	X		X	X	X
		RS.AN-2: The impact of the incident is understood	X	X	X	X			X	
		RS.AN-3: Forensics are performed	X	X	X	X			X	
		RS.AN-4: Incidents are categorized consistent with response plans	X	X	X	X			X	

Function	Category	Subcategory	PCI-DSS	CRR	CSET	BCEB	Stadium Guide	ISO 27001/2	COBIT	CSC
		RS.AN-5: Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g., internal testing, security bulletins, or security researchers)	X	X	X	X			X	
RESPOND (RS)	**Mitigation (RS.MI):** Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	**RS.MI-1:** Incidents are contained	X	X	X	X				
		RS.MI-2: Incidents are mitigated	X	X	X	X				
		RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	X	X	X	X				
RESPOND (RS)	**Improvements (RS.IM):** Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	**RS.IM-1:** Response plans incorporate lessons learned	X	X	X	X				
		RS.IM-2: Response strategies are updated	X	X	X	X				
RECOVER (RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity events.	**RC.RP-1:** Recovery plan is executed during or after a cybersecurity incident	X	X	X	X				
RECOVER (RC)	**Improvements (RC.IM):** Recovery planning and processes are improved by incorporating lessons learned into future activities.	**RC.IM-1:** Recovery plans incorporate lessons learned	X	X	X	X				
		RC.IM-2: Recovery strategies are updated	X	X	X	X				
RECOVER (RC)	**Communications (RC.CO):** Restoration activities are coordinated with internal and external parties (e.g., coordinating centers, Internet Service Providers, owners of attacking systems,	**RC.CO-1:** Public relations are managed		X	X	X				
		RC.CO-2: Reputation is repaired after an incident		X	X	X				

Function	Category	Subcategory	PCI-DSS	CRR	CSET	BCEB	Stadium Guide	ISO 27001/2	COBIT	CSC
	victims, other Computer Security Incident Response Teams [CSIRTs], and vendors).	**RC.CO-3:** Recovery activities are communicated to internal and external stakeholders as well as executive and management teams	X	X	X	X				

Appendix B: Notional-Use Case Study—Commercial Facilities Organization A

This notional-use case study is intended to serve as one example of how a Commercial Facilities Sector organization might implement the Framework.

Goal Level

Commercial Facilities Organization A seeks to use the Framework with a **strict** interpretation of the Implementation Guidance to improve its cybersecurity and risk management practices. The Framework is partially implemented, as Organization A adheres to a range of requirements from Federal and State laws.

Primary Actor, Stakeholders, and Interests

Commercial Facilities Organization A is a regional organization that operates three satellite locations with 300 employees. Stakeholders of the organization include employees, shareholders, and government regulators. Commercial Facilities Organization A is concerned with the resilience of its control systems. The security of the systems and information is essential to maintaining reliable operations. These security programs must have strong board and senior management level support, integration of security activities and controls throughout the organization's business processes, and clear accountability for carrying out security responsibilities.

Current Condition

Commercial Facilities Organization A reviews the Commercial Facilities Sector Cybersecurity Framework Implementation Guidance to understand the steps and informative resources associated with implementing the Framework. Commercial Facilities Organization A assesses its current cybersecurity profile. The assessment shows that Commercial Facilities Organization A is only loosely aligned with the Framework's Functions. As a result, the organization uses its risk management process and adherence to numerous information security-focused regulations to create its Target Profile that reflects the desired strict interpretation for each selected Framework Category. The Target Profile is based on the selection of the Functions, Categories, and Subcategories that are aligned with the organization's business requirements, risk tolerance, and resources.

Implementation

Commercial Facilities Organization A follows the recommended steps on how an organization can use the Framework to create a new cybersecurity program or improve an existing cybersecurity program.

- **Step 1: Identify**. Commercial Facilities Organization A identifies its mission objectives, describes cybersecurity risks, and determines which organizational components will use the Framework.
- **Step 2: Orient.** Commercial Facilities Organization A identifies the systems, assets, requirements, and risk management approaches and determines how to evaluate current risk management and cybersecurity posture.
- **Step 3: Create a Current Profile**. Beginning with the Categories specified in the Framework Core, Commercial Facilities Organization A develops a "Current Profile" that reflects its understanding of its present-day cybersecurity activities.
- **Step 4: Conduct a Risk Assessment**. Commercial Facilities Organization A analyzes the operational environment and determines that a cyberattack against its cyber infrastructure is likely over the long term based on information and resources available through CISA and other government partners. Based on its

risk assessment, Commercial Facilities Organization A identifies vulnerabilities and determines the consequence if those vulnerabilities are exploited.

- **Step 5: Create a Target Profile**. Commercial Facilities Organization A creates a Target Profile that focuses on the assessment of the Framework elements (e.g., Categories and Subcategories) describing the organization's desired cybersecurity outcomes.
- **Step 6: Determine, Analyze, and Prioritize Gaps**. Commercial Facilities Organization A compares the Current Profile and Target Profile to determine gaps and the resources necessary to address the gaps. Commercial Facilities Organization A creates a prioritized Action Plan that draws upon mission drivers, cost/benefit analysis, and understanding of risk to achieve Target Profile outcomes. Identifying gaps between the Current Profile and Target Profile allows for the creation of an Action Plan that Commercial Facilities Organization A implements to reduce its cybersecurity risk.
- **Step 7: Implement Action Plan**. The organization implements the steps defined in the Action Plan and monitors its current cybersecurity practices against the Target Profile.

Continuing to Adjust and Adapt

After implementing its plan, Commercial Facilities Organization A performs a self-evaluation against the Framework Implementation Tier 2 level before third-party validation of implementation. This self-evaluation includes determining the organization's defined, institutionalized, risk-informed, and management-approved processes and procedures. Although it is determined that Commercial Facilities Organization A complies with existing cybersecurity regulations, Commercial Facilities Organization A expresses its ultimate goal of being consistently secure throughout all of its processes.

Commercial Facilities Organization A also partners with a third party to evaluate the organization's management and execution of risk management activities. To move forward in a comprehensive manner, the organization leverages activities in Framework Core Functions mentioned in the Preconditions section.

Commercial Facilities Organization A strives to meet Tier 3, which includes regular and repeatable risk management processes to respond to a changing cybersecurity landscape. Tier 3 achievement is accomplished by overlaying the Framework and Commercial Facilities Organization A's risk management activities, gap identification, and mitigation. Risk management processes include risk-informed policies, processes, and procedures that are defined, implemented as intended, and validated.

[OPTION 1] The organization identifies areas for improvement based on Current Profile, Target Profile, and industry stakeholder input to focus on improving critical areas of cybersecurity and risk management:

- authentication,
- data analytics,
- cybersecurity workforce,
- privacy standards, and
- supply chain risk management.

[OPTION 2] The organization identifies key areas to consider for improvement within the Framework Core Functions, noted in **bold** below:

IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
• Asset Management • Business Environment • Governance • Risk Assessment • Risk Management Strategy	• Awareness and Training • Data Security • Information Protection Processes and Procedures • **Protective Technology**	• **Anomalies and Events** • **Security Continuous Monitoring** • **Detection Processes**	• **Response Planning** • **Communications** • Analysis • **Mitigation** • **Improvements**	• **Recovery Planning** • **Improvements** • **Communications**

Appendix C: Enhancing Existing Efforts

This Implementation Guidance was developed to be intrinsically backwards compatible, meaning it can be used to enhance the success of existing sector-specific programs and inform sector-level goals and guidelines. The resources below can also be used to increase knowledge and enhance cybersecurity practices.

- **Cybersecurity and Infrastructure Security Agency**: CISA leads the national effort to protect and enhance the resilience of the Nation's physical and cyber infrastructure. CISA's Industry Engagement website provides cybersecurity resources and best practices to assist businesses, government agencies, and other organizations in their efforts to use the Framework to manage their cyber risks as part of an all-hazards approach to enterprise risk management. Currently, there are many programs and resources available to critical infrastructure sectors and organizations that are looking to use the Framework and improve their cyber risk resilience. These resources are provided by CISA, other Federal and State agencies, and nonprofit organizations.
- **Commercial Facilities Sector-Specific Plan:** The *Commercial Facilities Sector-Specific Plan* (SSP) is designed to guide the sector's efforts to improve security and resilience and describe how the Commercial Facilities Sector manages risks and contributes to national critical infrastructure security and resilience, as set forth in Presidential Policy Directive 21 (PPD-21). The SSP reflects the overall strategic direction for the Commercial Facilities Sector and represents the progress made in addressing the sector's evolving risk, operating, and policy environments. As an annex to the *National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience* (NIPP 2013), this SSP tailors the NIPP's strategic guidance to the unique operating conditions and risk landscape of the Commercial Facilities Sector.

Table 7 provides specific information on how Framework use can help sector stakeholders address previously identified Commercial Facilities Sector priorities, as described in the resources above.

TABLE 7. How the Framework Addresses Commercial Facilities Sector Priorities

Sector Resource	Sector Strategy	How Framework Use Can Support the Strategy
Commercial Facilities SSP	States that it is a sector priority to conduct cyber and physical risk assessments and develop risk reduction strategies for evolving threats in collaboration with cross-sector, Federal, regional, and local security stakeholders.	The Framework encourages cyber risk assessments and the development of cybersecurity risk management strategies. For example, the Framework's Identify Function includes the categories Risk Assessment and Risk Management Strategy, which includes cybersecurity activities and outcomes for organizations to identify risks by assessing threats, vulnerabilities, likelihoods, and impacts (ID.RA-1, 2, and 5). It also has references for organizations to develop risk management strategies and communicate findings with stakeholders (ID.RA-3 and ID.RM-1).

Sector Resource	Sector Strategy	How Framework Use Can Support the Strategy
Commercial Facilities SSP	Acknowledges that the sector is "positioned to conduct a sector-wide cyber risk assessment" leveraging the critical functions and services identified in the Cyber-Dependent Infrastructure Identification (CDII).	The Framework introduces a seven-step process that organizations can use to create or improve their cybersecurity programs. The fourth step of this process, "Conduct a Risk Assessment," determines the likelihood of a cybersecurity event and potential impacts. Additionally, the Framework Core's Identify function is divided into Subcategories that address cyber risk assessments (ID.RA-1, 5, and 6) and cyber infrastructure identification (ID.AM-1-7).
	Acknowledges that "[r]isks associated with cyberattacks continue to grow, as Commercial Facilities Sector reliance on cyber systems, such as for online financial transactions and building management, rises" and identifies cyber risks as one of six major notable trends and emerging issues.	The Framework can help address risk by making stakeholders more aware of increasing cyber risks at a time when more organizations rely on cyber systems to conduct business. Further, it provides stakeholders a menu of tools and approaches to more effectively address risks.
	Sets a goal for Commercial Facilities Sector stakeholders to cost-effectively reduce cyber risks and enhance resilience.	The Framework, created through collaboration between government and the private sector, uses a common language to address and manage cybersecurity risk in a cost-effective way based on business needs without placing additional regulatory requirements on businesses. Regarding resilience, the Framework's Recover Function includes Categories and Subcategories dedicated to resilience activities.
	Calls for efforts to improve Commercial Facilities cybersecurity knowledge, tools, capabilities, risk assessments, and practices to secure critical physical and cyber assets linked to cyber systems.	The Framework Core is divided into Categories and Subcategories of cybersecurity outcomes closely tied to programmatic needs and particular activities. Many of these outcomes align to this SSP priority. Indeed, there are Subcategories for ensuring that organizations make sure employees understand their cybersecurity roles/responsibilities and are aware of expected data flows for users and systems (e.g., ID.GV-2, PR.AT-1, and DE.AE-1); carefully assess risks to physical and cyber assets (e.g., ID.RA-1-6); and adopt or improve asset management practices, including routine inventorying of hardware, devices, data, and software (e.g., ID.AM-1 and 2).
Commercial Facilities SSP	Encourages activities to enhance coordination with interdependent critical infrastructure sectors and community response partners to improve resilience and enhance decision-making.	The Framework's Implementation Tier 3 is defined, in part, as a level of cybersecurity sophistication at which an organization "understands its dependencies and partners and receives information from these partners that enables collaboration and risk-based management decisions within the organization in response to events." The Framework Core includes a Subcategory to ensure that an organization's place in critical infrastructure and its industry sector is identified and communicated (ID.BE-2). Moreover, the Core includes other Subcategories to ensure better coordination with internal and external partners in responding to and recovering from cybersecurity events (e.g., RS.CO-1-5).

Sector Resource	Sector Strategy	How Framework Use Can Support the Strategy
	Sets a priority for Commercial Facilities organizations to share security and resilience best practices and case studies to enable owners and operators to leverage lessons learned in all risk mitigation activities.	The Framework incorporates Subcategories that encourage cyber-related information sharing among internal and external stakeholders, including information about emerging threats and vulnerabilities (see ID.RA-2) and about the effectiveness of protection technologies (see PR.IP-8). There are also Subcategories emphasizing a lessons-learned approach for improving response and recovery practices (RS.IM and RC.IM-1). In fact, this approach of continuous learning and adaptation underlies the Framework document as a whole. As the Framework's Executive Summary explains: "The Framework is a living document [that] will continue to be updated and improved as industry provides feedback on implementation. As the Framework is put into practice, lessons learned will be integrated into future versions. This will ensure it is meeting the needs of critical infrastructure owners and operators in a dynamic and challenging environment of new threats, risks, and solutions."
	Promotes the work of the Commercial Facilities Cyber Working Group, which was established to help stakeholders gain insight into private sector cybersecurity needs and practices.	The Framework encourages stakeholders at all levels to collaborate on and coordinate development of cybersecurity standards, guidelines, and practices.
Commercial Facilities SSP	Encourages Commercial Facilities Sector organizations to continue working with DHS Office of Cybersecurity and Communications (CS&C) to improve cyber risk management efforts at the sector and individual facility level, including efforts to develop a long-term work plan related to cyber risk assessments.	The Framework's Profiles can serve as a good starting point for organizations seeking to develop new or update existing cybersecurity processes and practices, including risk assessment activities. Comparison of Profiles (e.g., the Current Profile and Target Profile) may reveal gaps to be addressed to meet cybersecurity risk management objectives, which could possibly compel an organization to write an action plan and/or roadmap to address these gaps. This risk-based approach enables an organization to gauge resource estimates (e.g., staffing and funding) to achieve cybersecurity goals in a cost-effective, prioritized manner.
	Establishes a number of sector research and development (R&D) priorities, including a priority to improve the ability of Commercial Facilities organizations to detect cyber threats and to identify and better understand potential impacts of a variety of cybersecurity failures.	The Framework's Core Functions, Categories, and Subcategories describe cybersecurity outcomes that address this particular R&D priority, including RS.AN-2 and DE.AE-4. To mitigate impacts, the Framework suggests that organizations consider investments in response/recovery planning and exercises.

Appendix D: Glossary

This appendix defines selected terms used in the publication.

TABLE 8. Framework Glossary

Buyer	The people or organizations that consume a given product or service.
Category	The subdivision of a Function into groups of cybersecurity outcomes, closely tied to programmatic needs and particular activities. Examples of Categories include "Asset Management," "Identity Management and Access Control," and "Detection Processes."
Critical Infrastructure	Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on cybersecurity, national economic security, national public health or safety, or any combination of those matters.
Cybersecurity	The process of protecting information by preventing, detecting, and responding to attacks.
Cybersecurity Event	A cybersecurity change that may have an impact on organizational operations (including mission, capabilities, or reputation).
Cybersecurity Incident	A cybersecurity event that has been determined to have an impact on the organization prompting the need for response and recovery.
Detect (function)	Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
Framework	A risk-based approach to reducing cybersecurity risk composed of three parts: the Framework Core, the Framework Profile, and the Framework Implementation Tiers. Also known as the "Cybersecurity Framework."
Framework Core	A set of cybersecurity activities and references that are common across critical infrastructure sectors and are organized around particular outcomes. The Framework Core comprises four types of elements: Functions, Categories, Subcategories, and Informative References.
Framework Implementation Tier	A lens through which to view the characteristics of an organization's approach to risk—how an organization views cybersecurity risk and the processes in place to manage that risk.
Framework Profile	A representation of the outcomes that a particular system or organization has selected from the Framework Categories and Subcategories.

Function	One of the main components of the Framework. Functions provide the highest level of structure for organizing basic cybersecurity activities into Categories and Subcategories. The five functions are Identify, Protect, Detect, Respond, and Recover.
Identify (function)	Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
Informative Reference	A specific section of standards, guidelines, and practices common among critical infrastructure sectors that illustrates a method to achieve the outcomes associated with each Subcategory. An example of an Informative Reference is ISO/IEC 27001 Control A.10.8.3, which supports the "Data-in-transit is protected" Subcategory of the "Data Security" Category in the "Protect" function.
Mobile Code	A program (e.g., script, macro, or other portable instruction) that can be shipped unchanged to a heterogeneous collection of platforms and executed with identical semantics.
Protect (function)	Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
Privileged User	A user that is authorized (and, therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.
Recover (function)	Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.
Respond (function)	Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
Risk	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.
Risk Management	The process of identifying, assessing, and responding to risk.
Risk Management Plan (RMP)	The Risk Management Plan outlines the identified process of risk management.
Subcategory	The subdivision of a Category into specific outcomes of technical and/or management activities. Examples of Subcategories include "External information systems are catalogued," "Data-at-rest is protected," and "Notifications from detection systems are investigated."
Supplier	Product and service providers used for an organization's internal purposes (e.g., IT infrastructure) or integrated into the products of services provided to that organization's Buyers.
Taxonomy	A scheme of classification.