NIST Interagency Report
NIST IR 8576 ipd

Transit Cybersecurity Framework Community Profile

Initial Public Draft

CheeYee Tang
Alex Alshtein
Eileen Division
Matt Hardison
Emma Holt
Christina Sames
Hillary Tran*

**Former employee; all work for this publication was done while at employer.*

This publication is available free of charge from:
https://doi.org/10.6028/NIST.8576.ipd

NATIONAL INSTITUTE OF
STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST Interagency Report
NIST IR 8576 ipd

Transit Cybersecurity Framework Community Profile

Initial Public Draft

CheeYee Tang
Smart Connected Systems Division
Communications Technology Laboratory

Alex Alshtein
Eileen Division
Matt Hardison
Emma Holt
Christina Sames
Hillary Tran*
The MITRE Corporation

**Former employee; all work for this publication was done while at employer.*

This publication is available free of charge from:
https://doi.org/10.6028/NIST.8576.ipd

January 2026

U.S. Department of Commerce
Howard Lutnick, Secretary

National Institute of Standards and Technology
Craig Burkhardt, Acting Under Secretary of Commerce for Standards and Technology and Acting NIST Director

Certain equipment, instruments, software, or materials, commercial or non-commercial, are identified in this paper in order to specify the experimental procedure adequately. Such identification does not imply recommendation or endorsement of any product or service by NIST, nor does it imply that the materials or equipment identified are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at https://csrc.nist.gov/publications.

How to Cite this NIST Technical Series Publication
Tang CE, Alshtein A, Division E, Hardison M, Holt E, Sames C, Tran H (2026) Transit Cybersecurity Framework Community Profile. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Internal Report (IR) NIST IR 8576. https://doi.org/10.6028/NIST.8576.ipd

Author ORCID iDs
CheeYee Tang: 0009-0000-2847-1443
Alex Alshtein: 0009-0009-9071-160X
Eileen Division: 0009-0004-3152-3776
Matt Hardison: 0009-0002-7422-8131
Emma Holt: 0009-0001-8269-4143
Christina Sames: 0009-0003-1817-8333
Hillary Tran: 0009-0000-7003-5506

Public Comment Period
January 22, 2026 – February 23, 2026

Submit Comments
transit-nccoe@nist.gov

National Institute of Standards and Technology
Attn: Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000

Additional Information
Additional information about this publication is available at https://csrc.nist.gov/pubs/ir/8576/ipd, including related content, potential updates, and document history.

All comments are subject to release under the Freedom of Information Act (FOIA).

Abstract

This document is a Cybersecurity Framework (CSF) Community Profile developed to support United States-based transit agencies. This “Transit Profile” is aligned with transit sector priorities and best practices and can be used as a guide for prioritizing cybersecurity activities and outcomes or as a starting point for building a new program. The Transit Profile was developed to complement, not replace, any existing cybersecurity programs, guidelines, or policies that transit agencies may rely on or have in place.

Keywords

Bus, commuter rail, cybersecurity, Cybersecurity Framework (CSF), operational technology (OT), public transportation, rail, risk management, subway, transit.

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation’s measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL’s responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems. The Special Publication 800-series reports on ITL’s research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

Note to Reviewers

NIST is particularly interested in feedback on:

- Does this Community Profile appropriately reflect the cybersecurity challenges and priorities of the transit community?
- How do you envision using this guide? What changes would you like to see to increase usability and effectiveness?
- Are the designations of a Framework Subcategory as “Elevated” or “Supporting” appropriate?
- Are the terms “Elevated” and “Supporting” understood and clearly defined?
- Are the rationales provided for the “Elevated” Subcategories appropriate and is the link to transit clear?

Call for Patent Claims

This public review includes a call for information on essential patent claims (claims whose use would be required for compliance with the guidance or requirements in this Information Technology Laboratory (ITL) draft publication). Such guidance and/or requirements may be directly stated in this ITL Publication or by reference to another publication. This call also includes disclosure, where known, of the existence of pending U.S. or foreign patent applications relating to this ITL draft publication and of any relevant unexpired U.S. or foreign patents.

ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in written or electronic form, either:

a) assurance in the form of a general disclaimer to the effect that such party does not hold and does not currently intend holding any essential patent claim(s); or

b) assurance that a license to such essential patent claim(s) will be made available to applicants desiring to utilize the license for the purpose of complying with the guidance or requirements in this ITL draft publication either:

    i. under reasonable terms and conditions that are demonstrably free of any unfair discrimination; or

    ii. without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination.

Such assurance shall indicate that the patent holder (or third party authorized to make assurances on its behalf) will include in any documents transferring ownership of patents subject to the assurance, provisions sufficient to ensure that the commitments in the assurance are binding on the transferee, and that the transferee will similarly include appropriate provisions in the event of future transfers with the goal of binding each successor-in-interest.

The assurance shall also indicate that it is intended to be binding on successors-in-interest regardless of whether such provisions are included in the relevant transfer documents.

Such statements should be addressed to: transit-nccoe@nist.gov

Table of Contents

List of Tables

List of Figures

Acknowledgments

The Transit Profile was developed based on feedback from federal agencies, industry organizations, and stakeholders of small, medium, and large transit agencies across the United States. We appreciate the contributions and valuable insights of representatives from the following organizations (listed alphabetically):

Federal Government

- U.S. Department of Homeland Security Transportation Security Administration (TSA)
- U.S. Department of Transportation (DOT) Federal Railroad Administration (FRA)
- U.S. DOT Federal Transit Administration (FTA)
- U.S. DOT Office of the Chief Information Officer

National Industry and Research Organizations

- American Public Transportation Association (APTA)
- Community Transportation Association of America (CTAA)
- Mineta Transportation Institute

Transit Agencies

- Bay Area Rapid Transit (BART) (San Francisco, California)
- Capital Metro (CapMetro) (Austin, Texas)
- Central Ohio Transit Authority (COTA) (Columbus, Ohio)
- Foothill Transit (West Covina, California)
- MARTA (Atlanta, Georgia)
- Mendocino Transit (Ukiah, California)
- Metra (Chicago, Illinois)
- Metropolitan Transportation Authority (MTA) (New York, New York)
- Monterey-Salinas Transit (Monterey, California)
- Prairie Hills Transit (Spearfish, South Dakota)
- Regional Transportation District (RTD) (Denver, Colorado)
- Rogue Valley Transit (Medford, Oregon)
- SamTrans (San Carlos, California)
- South Shore Line (South Bend, Indiana)
- Virginia Railway Express (VRE) (Virginia)

Executive Summary

The Transit Cybersecurity Framework (CSF) Community Profile ("Transit Profile") is a voluntary, risk-based guide designed to help U.S. transit agencies enhance cybersecurity while maintaining safe and efficient transit services. Built on the National Institute of Standards and Technology (NIST) CSF 2.0, it translates transit mission needs into a baseline of cybersecurity outcomes that transit agencies can adopt and tailor to their unique operational environments.

Transit agencies operate complex networks of business and operational systems, such as rail signaling, bus charging, scheduling, ticketing, and public information systems. The transition to digital, network-based communication has expanded the cyber attack surface, requiring agencies to manage cybersecurity risks alongside safety and operational demands. To address these challenges, the Transit Profile focuses on three strategic priorities: securing and managing critical assets to ensure safe and reliable operations, fostering collaboration with stakeholders and suppliers to enhance resilience and supply chain security, and continuously improving organizational processes and workforce cybersecurity awareness and capabilities.

The Transit Profile can help transit agencies focus resources on cybersecurity activities aligned with these strategic priorities by mapping them to relevant CSF Subcategories. This enables transit leaders to prioritize cybersecurity capabilities, perform gap analyses, and make informed decisions. The Profile integrates industry-specific cybersecurity considerations and guidelines for agencies of all sizes, including small- and medium-sized transit agencies (SMTAs) with limited resources, and supports scalable actions based on size and maturity. The Profile can enhance existing cybersecurity programs, helping agencies adopt best practices, establish a shared taxonomy for discussing cybersecurity risk with leadership, plan strategically, and communicate cybersecurity needs to stakeholders, suppliers, and funding entities.

The Profile is intended to complement, not replace, existing programs, standards, and regulatory obligations. As a non-regulatory and neutral entity, NIST developed the Transit Profile in collaboration with the transit community to provide cybersecurity considerations and guidelines tailored to the sector's unique challenges. By working closely with transit operators, federal agencies, and other stakeholders, NIST ensures the Profile reflects industry needs while supporting voluntary adoption of cybersecurity best practices.

1. Introduction

The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0 introduced the concept of a *Community Profile*. A Community Profile is a baseline of CSF cybersecurity outcomes that is created and published to address shared interests and goals among a number of organizations. It is typically developed for a particular sector, subsector, technology, threat type, or other use case, and can be used by an organization as the basis for its own Organizational Target Profile [CSF2.0].

NIST developed the Transit Profile to provide a voluntary, risk-based approach for managing cybersecurity activities, reducing cybersecurity risks, and improving the cybersecurity posture of the transit community.

1.1. Purpose and Scope

This document represents a CSF Community Profile that describes shared interests, goals, and outcomes for mitigating cybersecurity risk within the transit community. Transit agencies, as defined in this Profile, include owners and operators of public transportation services, including bus and transit rail systems (e.g., light rail, subway, commuter rail), as well as affiliated entities such as county governments overseeing and/or funding transit operations.

The Transit Profile suggests prioritization of cybersecurity outcomes to meet specific strategic business/mission focus areas for the transit community and identifies relevant and actionable security practices that can be implemented in support of those areas. It is intended to complement, not replace, any existing cybersecurity programs, guidelines, or policies that transit agencies may already have in place.

The Transit Community Profile:

- Describes a shared taxonomy to support communication about cybersecurity risk management for transit owners/operators
- Offers a framework to aggregate transit cybersecurity considerations and guidelines from multiple industry resources
- Develops common target outcomes that transit owners and operators can use to support strategic planning efforts and cybersecurity assessments
- Assists in identifying and communicating cybersecurity needs to the broader transit community of suppliers, operating partners, and funding entities
- Provides scalable and achievable cybersecurity considerations and guidelines for transit owners/operators of all sizes

1.2. Audience

This document focuses on cybersecurity considerations specific to transit agencies and assumes readers have a foundational understanding of operational technology (OT) and general information technology (IT) security concepts. The intended audience includes:

- Control engineers, integrators, system suppliers, and architects involved in designing or implementing secure transit systems.
- System and network administrators, cybersecurity professionals, physical security personnel, and OT operators responsible for managing, patching, or securing transit systems.
- Executives and management teams overseeing transit operations.
- Senior security officials evaluating cyber risks and implementing cybersecurity programs to support transit operations.
- Affiliated entities, such as federal agencies and county governments that oversee and/or fund transit agencies.
- Transit industry associations and researchers seeking to understand the unique cybersecurity needs of transit systems.

1.3. Document Structure

The remainder of the Transit Profile is divided into the following sections:

- Section 2 provides a summary of challenges to securing transit systems.
- Section 3 provides an overview of the NIST CSF 2.0.
- Section 4 describes the Transit Profile development methodology.
- Section 5 provides the transit sector-specific rationale, guidelines, and considerations for prioritized CSF Subcategories.
- References provide a list of references used in the development of this document.
- Appendix A provides a selected bibliography of resources used to inform the Profile.
- Appendix B provides a complete listing of all CSF Subcategory designations.
- Appendix C provides a list of acronyms and abbreviations used in this document.

2. Challenges to Securing Transit Systems

Transit agencies manage a complex network of business and operational systems in service to their mission. Examples can include:

- Rail signaling and train control systems
- Bus fueling, battery-electric charging, and charge management systems
- Scheduling and dispatching
- Facility management systems
- Emergency communications systems
- Control and communication systems
- Ticketing systems
- Command centers
- Revenue collection systems, including back office and fare payment systems
- Public information systems, such as station-based electronic signage and web and mobile applications/systems

Traditionally, many of these systems relied on direct connections for communications. Today, communication between and among these systems is digital and network-based, including through the extensive use of wireless connectivity. This dependence on digital technology and interconnections to sustain daily operations has widened the cyber attack surface for transit agencies. Operators must now manage the cybersecurity risk of their IT and OT systems while meeting increasingly demanding safety and operating requirements.

Several aspects of the transit sector make it uniquely challenging to protect and require a more tailored approach to prioritize and apply cybersecurity risk management measures. These include:

- **Safety-centric culture**. A transit agency’s top responsibility is safety. Cybersecurity knowledge and awareness in many agencies is still maturing. The American Public Transportation Association (APTA), federal agencies, suppliers, and the operating agencies themselves have worked to develop and organize resources to advance cybersecurity awareness and protections specific to transit operations. Cybersecurity measures and training must continue to be integrated into an agency’s overall safety framework to improve effectiveness.
- **Safety-critical control systems**. Safety-critical control systems—such as signaling and train control for rail, and steering, acceleration, and brake control for buses—are governed by standards which may not fully account for cybersecurity risk. Cybersecurity risk mitigations for these systems must be carefully implemented to ensure they meet safety and industry standards without triggering the need for safety recertification.

- **Long-lived and legacy systems**. Most transit agencies simultaneously manage both modern and legacy IT and OT infrastructure and systems. Many systems and assets in the transit sector have long lifecycles measured in decades, not years, and may not be able to accommodate modern cybersecurity controls (e.g., multifactor authentication (MFA), advanced encryption). This is evident in legacy systems and also applies to long-lived OT systems that are remote, difficult to access, or challenging to update. Retrofitting these systems for cybersecurity purposes can be cost-prohibitive and disruptive, and compensating cybersecurity controls may be needed to meet security outcomes.
- **Communication systems**. Communication systems (e.g., Wi-Fi, radio, cellular, satellite, wired) are the backbone of public transit operations, supporting coordination between buses, vehicles, trains, control centers, and infrastructure. They facilitate real-time updates, signaling, dispatching, and monitoring. Any disruption or compromise of these systems can lead to operational failures and delays, adversely affecting the safety and reliability of transit systems.
- **Vendor supply chain**. Transit agency systems and components are supplied by a large variety of domestic and global suppliers. Likewise, transit agencies rely heavily on vendor services and contractors to install, manage, and maintain their IT and OT systems and infrastructure. Cybersecurity supply chain risk management must be part of an organization-wide risk management strategy.
- **Distributed and mobile operations**. Transit operations and their support systems are geographically dispersed with rolling stock. Rail operators, for example, manage systems and sensors that encompass the rail network and associated facilities. Likewise, bus operators support moving assets, garages, and maintenance facilities that are deployed across a metropolitan region.
- **Physical security concerns**. Transit assets and infrastructure are both accessible to and used by the public. Many of the supporting systems are also distributed across a broad region, making physical security more challenging and exposing certain elements, such as telecommunications systems or wayside equipment, to potential unauthorized physical and logical access by malicious actors.
- **Funding.** Transit agencies, as public sector entities, generally rely on subsidies to cover their capital and operating costs. This creates a unique challenge in obtaining the necessary funds to implement and manage cybersecurity measures for protecting their systems. While agencies can pursue a variety of funding sources, such as capital funding, operating funding, and grant funding, these sources must address multiple competing priorities. Additionally, even when funding is approved, it typically involves a lengthy authorization process, making it difficult to secure resources for cybersecurity needs. This unpredictability and long lead time can work against efforts to address cybersecurity needs promptly.

3. Overview of the NIST Cybersecurity Framework

This Community Profile is based on the NIST CSF 2.0 [CSF 2.0], which provides a flexible and risk-based approach to managing cybersecurity.

The CSF helps organizations of any size, sector, or level of cyber maturity address their unique cybersecurity risks while improving communication and collaboration across stakeholders. For the transit sector, the CSF provides a foundation to:

- Establish a common understanding of cybersecurity risks, threats, and priorities.
- Align on desired outcomes and target states for cybersecurity practices.
- Identify and prioritize opportunities for improvement in a consistent, repeatable manner.
- Support cross-organization communication and coordination to manage cybersecurity risk effectively.

The CSF Core is a taxonomy of high-level cybersecurity outcomes that can help organizations manage their cybersecurity risks. The Core components are a hierarchy of Functions, Categories, and Subcategories that detail each outcome. These outcomes can be understood by a broad audience, including executives, managers, and practitioners, regardless of their cybersecurity expertise [CSF 2.0].

The CSF Core Functions (Govern, Identify, Protect, Detect, Respond, and Recover) organize cybersecurity outcomes at their highest level. The Core then identifies underlying key Categories and Subcategories for each Function [CSF 2.0]. The six Functions of the CSF 2.0 Core are composed of 22 Categories, which are further broken down into 106 Subcategories of more specific outcomes.

Section 5 provides more detailed information on each Function, Category, and Subcategory as part of defining the Community Profile. Additionally, NIST provides supplemental resources to help organizations understand, adopt, and use CSF 2.0 and achieve the desired outcome of each Subcategory, including Implementation Examples and Informative References. The NIST CSF website contains the most current information regarding available Implementation Examples and Informative References. Communities and organizations can choose to add their own Implementation Examples and Informative References that are unique to their transit environment in the future.

3.1. Govern (GV)

The organization’s cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.

Table 1. Govern (GV) Cybersecurity Framework Categories

Category	Cybersecurity Outcome
GV.OC	The circumstances—mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements—surrounding the organization's cybersecurity risk management decisions are understood
GV.RM	The organization's priorities, constraints, risk tolerance and appetite statements, and assumptions are established, communicated, and used to support operational risk decisions
GV.RR	Cybersecurity roles, responsibilities, and authorities to foster accountability, performance assessment, and continuous improvement are established and communicated
GV.PO	Organizational cybersecurity policy is established, communicated, and enforced
GV.OV	Results of organization-wide cybersecurity risk management activities and performance are used to inform, improve, and adjust the risk management strategy
GV.SC	Cyber supply chain risk management processes are identified, established, managed, monitored, and improved by organizational stakeholders

3.2. Identify (ID)

The organization's current cybersecurity risks are understood.

Table 2. Identify (ID) Cybersecurity Framework Categories

Category	Cybersecurity Outcome
ID.AM	Assets (e.g., data, hardware, software, systems, facilities, services, people) 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.RA	The cybersecurity risk to the organization, assets, and individuals is understood by the organization
ID.IM	Improvements to organizational cybersecurity risk management processes, procedures and activities are identified across all CSF Functions

3.3. Protect (PR)

Safeguards to manage the organization's cybersecurity risk are used.

Table 3. Protect (PR) Cybersecurity Framework Categories

Category	Cybersecurity Outcome
PR.AA	Access to physical and logical assets is limited to authorized users, services, and hardware and managed commensurate with the assessed risk of unauthorized access
PR.AT	The organization's personnel are provided with cybersecurity awareness and training so that they can perform their cybersecurity-related tasks
PR.DS	Data are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information
PR.PS	The hardware, software (e.g., firmware, operating systems, applications), and services of physical and virtual platforms are managed consistent with the organization's risk strategy to protect their confidentiality, integrity, and availability
PR.IR	Security architectures are managed with the organization's risk strategy to protect asset confidentiality, integrity, and availability, and organizational resilience

3.4. Detect (DE)

Possible cybersecurity attacks and compromises are found and analyzed.

Table 4. Detect (DE) Cybersecurity Framework Categories

Category	Cybersecurity Outcome
DE.CM	Assets are monitored to find anomalies, indicators of compromise, and other potentially adverse events
DE.AE	Anomalies, indicators of compromise, and other potentially adverse events are analyzed to characterize the events and detect cybersecurity incidents

3.5. Respond (RS)

Actions regarding a detected cybersecurity incident are taken.

Table 5. Respond (RS) Cybersecurity Framework Categories

Category	Cybersecurity Outcome
RS.MA	Responses to detected cybersecurity incidents are managed
RS.AN	Investigations are conducted to ensure effective response and support forensics and recovery activities
RS.CO	Response activities are coordinated with internal and external stakeholders as required by laws, regulations, or policies
RS.MI	Activities are performed to prevent expansion of an event and mitigate its effects

3.6. Recover (RC)

Assets and operations affected by a cybersecurity incident are restored.

Table 6. Recover (RC) Cybersecurity Framework Categories

Category	Cybersecurity Outcome
RC.RP	Restoration activities are performed to ensure operational availability of systems and services affected by cybersecurity incidents
RC.CO	Restoration activities are coordinated with internal and external parties

4. Transit Profile Development Methodology

Developing a Community Profile involves active participation and collaboration from community stakeholders. The NIST National Cybersecurity Center of Excellence (NCCoE) engaged with representatives from key federal agencies and national organizations (listed below) to identify a cross section of small, medium, and large transit agencies to take part in a series of Community Profile working sessions.

Federal Agencies:

- U.S. Department of Homeland Security Transportation Security Administration (TSA)
- U.S. Department of Transportation (DOT) Federal Railroad Administration (FRA)
- U.S. DOT Federal Transit Administration (FTA)
- U.S. DOT Office of the Chief Information Officer

National Industry and Research Organizations:

- American Public Transportation Association (APTA)
- Community Transportation Association of America (CTAA)

During these working sessions, transit agency representatives (see Acknowledgements for a complete list) took part in facilitated discussions and tailored activities designed to gather and consolidate information and perspectives on their unique cybersecurity challenges, mission priorities, organizational capabilities and resources, and general insights and expertise to inform the Community Profile.

In these discussions, transit community participants:

- Identified high-level community priorities based on importance/criticality to the transit community and its operations
- Discussed ranked cybersecurity outcomes that enable each transit community priority
- Shared their expertise, challenges, perspectives, and expectations to enrich the Community Profile and ensure that it addresses the specific threats and vulnerabilities unique to the transit sector
- Shared key transit-specific cybersecurity resources and guidance, including APTA's Cybersecurity Resources, FTA's Cybersecurity Resources for Transit Agencies, and TSA's Surface Transportation Cybersecurity Toolkit to inform Profile development

The team used insights from this process to create NIST Cybersecurity White Paper (CSWP) 51 ipd, *Developing a Transit Cybersecurity Framework Community Profile: Project Update*, which outlines key industry challenges, themes, and preliminary Transit Profile content. The white paper was released publicly to allow industry participants and the general public to review preliminary findings and provide input on transit priorities, challenges, and recommendations. Feedback gathered through this process was incorporated into the Profile.

4.1. Transit Sector Strategic Focus Areas

The Profile was developed considering common strategic focus areas for transit agencies. The strategic focus areas are made up of the business/mission priorities that the community identified during working sessions and through public feedback. These strategic focus areas provide the necessary context for identifying and managing applicable cybersecurity risk mitigation measures. Three common strategic focus areas identified by the transit community were initially identified along with key cybersecurity practices for supporting each of the community's business/mission priorities. This information allows users to better prioritize actions and resources according to their defined needs. While the three strategic focus areas each address transit-specific cybersecurity risk from a different angle, they share common elements and mutually reinforce one another.

The strategic focus areas are not listed in priority order.

Strategic Focus Area 1: Secure and Manage Critical Assets

A top priority of agencies across the United States is to ensure safe, efficient, and reliable operations. Within Strategic Focus Area 1, this extends to:

- **Delivering Safe, Efficient, and Reliable Transit**: Ensure safety, efficiency, and resilience in transit operations by identifying and protecting critical assets, monitoring for threats, maintaining business continuity, and complying with safety regulations.
- **Protecting Data**: Safeguard sensitive information and financial systems and comply with data protection laws.
- **Protecting IT/OT Systems and Assets**: Maintain asset inventories, secure legacy and communication systems, protect physical and remote assets, and leverage modern cybersecurity solutions without compromising safety.

Strategic Focus Area 2: Collaborate with Partners and Suppliers

Effective cybersecurity in transit agencies depends on strong collaboration and consensus among internal and external stakeholders. Within Strategic Focus Area 2, this includes:

- **Fostering Collaboration Among Stakeholders**: Align cybersecurity goals with stakeholder needs, define roles and responsibilities, and support incident response and recovery.
- **Delivering Reliable "On Time" Service**: Coordinate with internal and external partners to maintain and/or restore services during disruptions by implementing robust disaster recovery and continuity planning, ensuring resilience in both routine and emergency operations.
- **Securing the Transit Supply Chain**: Manage risks from vendors and suppliers, integrate cybersecurity into procurement, and plan for equipment replacement to ensure business continuity.

Strategic Focus Area 3: Continuously Improve the Organization and Workforce

Building a resilient transit organization requires ongoing investment in people, processes, and technology. Within Strategic Focus Area 3, this encompasses:

- **Engaging in Continuous Improvement of Transit Operations**: Evaluate and secure new/emerging technologies, enhance operational efficiency, and apply lessons learned to strengthen cybersecurity.
- **Cultivating a Cyber Aware Workforce**: Train back office and frontline staff, integrate cybersecurity into enterprise risk management, and promote awareness and accountability.

4.2. Prioritization Process

The considerations and priority of each Subcategory were determined based on observations in the field, subject matter expertise, and input from stakeholders during working sessions and public comment on CSWP 51. The NCCoE team of transit sector and cybersecurity subject matter experts (SMEs) analyzed outputs from the CSF Profile working sessions, strategic focus areas, community priorities, and CSF Category prioritization activities with stakeholders. Analysis of stakeholder input and contributions informed the selection and prioritization of CSF Subcategories in the Transit Profile by the NCCoE team.

The Transit Profile offers proposed Subcategory priorities to assist transit agencies in identifying which Subcategories they may wish to address sooner. The priorities are not intended to reflect the degree of difficulty for achieving the Subcategory. The priority level of Subcategories may be higher or lower for individual transit agencies based on their unique environment, needs, risk tolerance, and other factors. The proposed Subcategory priority is indicated in each Table using the following designations:

- **Elevated (E)**: These Subcategories are considered the most critical to address the challenges for a Strategic Focus Area, as communicated by the stakeholders. They should typically be addressed first, based on available resources.
- **Supporting (—)**: These Subcategories are generally important to a Strategic Focus Area but are generally less urgent than Elevated Subcategories. The “Supporting” designation does not imply a Subcategory should be excluded or is unnecessary; rather, these Subcategories should be addressed based on available resources and risk considerations.

For clarity and usability, only Subcategories labeled as “Elevated” are included in the Profile mapping in Section 5. Appendix B provides a complete list of both Elevated and Supporting designations for all CSF Subcategories across each strategic focus area.

Transit agencies are encouraged to develop strategies that address all CSF 2.0 Subcategories as part of a comprehensive cybersecurity program. Prioritizations offered in the Transit Profile highlight cybersecurity outcomes that can have the greatest impact on addressing transit-related challenges within each strategic focus area.

It is important to note that Subcategory designations in the Profile are relative and may differ for individual transit agencies. Agencies should consider their specific goals, priorities, and risk tolerances when applying the Profile and tailor its use to their unique context. Trade-offs for mitigation strategies may vary depending on an agency's environment and circumstances.

4.3. Agency Size and Risk Management

Discussions with transit stakeholders revealed that differences in agency size can shape cyber risk management priorities and challenges. While both large and small agencies face financial pressures, the source of those pressures and the priorities differ. Smaller and rural agencies, for example, often operate with limited technical and financial resources, requiring staff to operate in multiple roles and rely on vendor-supplied and -supported solutions. While their smaller scale allows for quicker response and closer coordination between IT and OT teams, these agencies face challenges in implementing and managing advanced cybersecurity controls while also delivering comprehensive cybersecurity systems governance, oversight, and consistent training.

In contrast, larger agencies often benefit from dedicated technical staff and greater resources, but at the same time must contend with complex, geographically dispersed systems and extensive legacy infrastructure investments. These agencies therefore often face challenges managing cybersecurity programs across large regions and with outdated or difficult-to-maintain systems.

This diversity makes protecting the transit sector particularly challenging as solutions must be tailored to each agency's unique characteristics and priorities. Regardless of size, all transit agencies must balance operational needs with cybersecurity risks.

This Transit Profile is designed to help agencies of all sizes reduce and better manage their cybersecurity risks. It does so by exploring the full spectrum of priorities and risks and identifying key considerations for each, so that each agency can align their plans with their own specific circumstances. It is also designed to complement, not replace, existing cybersecurity standards and industry guidelines already in use by transit agencies. As such, the discussion of Subcategory considerations and guidelines include citations to the many references and resources available to the industry. In short, the Transit Profile is not a one-size-fits-all solution for managing cybersecurity risk but is designed to help agencies identify activities essential to critical service delivery and prioritize investments to maximize the effectiveness of their resources.

5. The Transit Profile

Tables 7-12 below use the CSF Core to summarize transit-related considerations and guidelines, where relevant, for those CSF Subcategories designated as Elevated (indicated as a bold "E") within at least one of the three strategic focus areas for the transit sector. Each table addresses a single CSF Function. To support usability, only Subcategories marked as "Elevated" are included in Tables 7-12. Appendix B provides a complete list of all "Elevated" and "Supporting" CSF Subcategory designations for each strategic focus area.

Each table contains the following columns (depicted in Figure 1: How to Read the Transit Profile Tables 7-12):

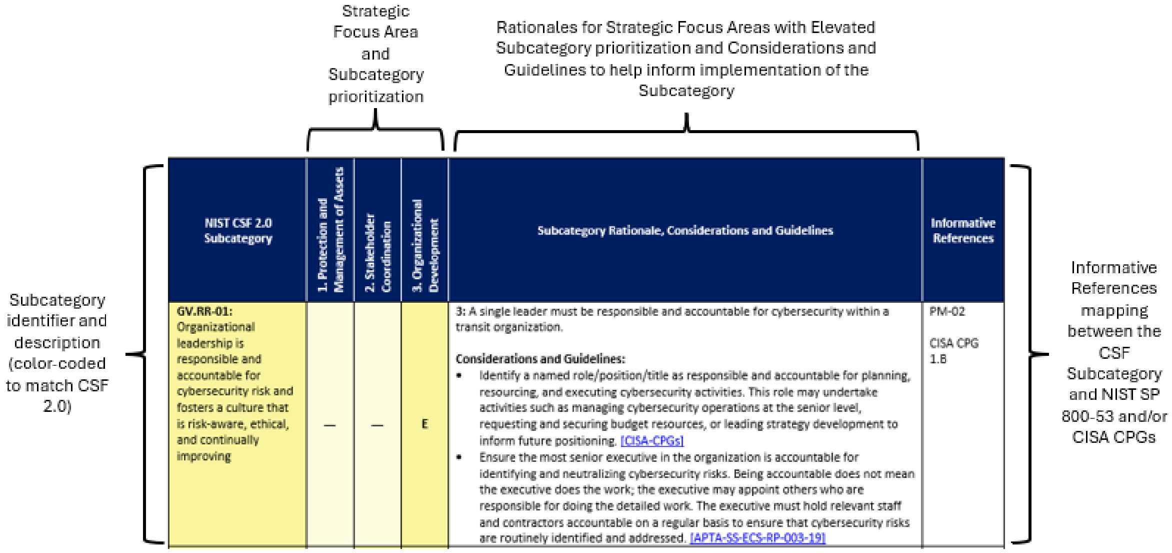
- **NIST CSF 2.0 Subcategory:** Lists the unique identifier and description of the CSF Subcategory.
- **Strategic Focus Area and Subcategory Priorities:** Indicates the priority level (as described earlier) for each strategic focus area, indicating how important it may be for a transit agency to achieve the Subcategory's outcome(s) to meet the objective of each strategic focus area.
- **Subcategory Rationale, Considerations, and Guidelines:** Contains the following**:**
  - **Bold Number** (i.e., 1, 2, 3) **and Rationale:** Identifies Subcategories prioritized as "Elevated" for a Strategic Focus Area, with the bold number indicating alignment to a strategic focus area(s). The rationale explains the importance of a Subcategory in relation to a strategic focus area. These rationales may reflect stakeholder input shared during working sessions and public feedback on CSWP 51.
  - **Considerations and Guidelines**: Provides non-comprehensive recommendations to help transit agencies achieve the outcomes of the Subcategory, relevant to the strategic focus area. Considerations are informed by observations in the field and subject matter expertise. Guidelines provide context for implementing a CSF Subcategory in support of a strategic focus area consistent with existing transit cybersecurity resources such as APTA standards, NIST publications, and Cybersecurity and Infrastructure Security Agency (CISA) Cross-Sector Cybersecurity Performance Goals (CPGs) [CISA-CPGs] that transit agencies may already be using.
  - **Informative References:** Includes mappings to publicly available and applicable resources (e.g., laws, standards, guidelines). These mappings reference a relevant[1] subset of NIST SP 800-53 Revision 5 [SP800-53r5][2] security controls and CISA CPGs [CISA-CPGs] for each Elevated Subcategory. These references can assist transit agencies in achieving Subcategory outcomes and understanding

[1] Only those NIST SP 800-53 security controls and CISA CPGs that align with community feedback and are informed by a Subcategory rationale, and expert insights and experience are included as Informative References.

[2] The mapping between CSF 2.0 and NIST SP 800-53, Rev 5, as available at: https://csrc.nist.gov/projects/olir/informative-reference-catalog/details?referenceId=131#/ (last accessed 12/22/2025).

alignment with existing transit resources. Agencies can also use these references to identify where they may already meet the outcomes. (*NOTE: NIST acknowledges that the International Electrotechnical Commission (IEC) is developing an international standard for railway cybersecurity (i.e., IEC 63452). Once finalized, NIST may review and consider incorporating IEC 63452 into the Profile in future updates.*)

Fig. 1. How to Read the Transit Profile Tables 7-12


Strategic Focus Area and Subcategory prioritization
Rationales for Strategic Focus Areas with Elevated Subcategory prioritization and Considerations and Guidelines to help inform implementation of the Subcategory
Subcategory identifier and description (color-coded to match CSF 2.0)
Informative References mapping between the CSF Subcategory and NIST SP 800-53 and/or CISA CPGs

NIST CSF 2.0 Subcategory	1. Protection and Management of Assets	2. Stakeholder Coordination	3. Organizational Development	Subcategory Rationale, Considerations and Guidelines	Informative References
GV.RR-01: Organizational leadership is responsible and accountable for cybersecurity risk and fosters a culture that is risk-aware, ethical, and continually improving	—	—	E	**3:** A single leader must be responsible and accountable for cybersecurity within a transit organization. **Considerations and Guidelines:** • Identify a named role/position/title as responsible and accountable for planning, resourcing, and executing cybersecurity activities. This role may undertake activities such as managing cybersecurity operations at the senior level, requesting and securing budget resources, or leading strategy development to inform future positioning. [CISA-CPGs] • Ensure the most senior executive in the organization is accountable for identifying and neutralizing cybersecurity risks. Being accountable does not mean the executive does the work; the executive may appoint others who are responsible for doing the detailed work. The executive must hold relevant staff and contractors accountable on a regular basis to ensure that cybersecurity risks are routinely identified and addressed. [APTA-SS-ECS-RP-003-19]	PM-02 CISA CPG 1.B

5.1. Govern

Table 7. Subcategory-level Guidelines for the Govern Function

NIST CSF 2.0 Subcategory	1. Protection and Management of Assets	2. Stakeholder Coordination	3. Organizational Development	Subcategory Rationale, Considerations, and Guidelines	Informative References
GV.OC-01: The organizational mission is understood and informs cybersecurity risk management	E	—	E	**1:** Cybersecurity is an enterprise risk that senior leaders should consider alongside others, such as operational, financial and reputational risk. A transit agency's mission and vision inform and help prioritize cybersecurity risk management decisions related to safe and reliable transit services, and the need for, or use of, new technologies. **3**: Understanding the transit operator's mission helps identify and prioritize the groups or functional areas where cybersecurity training and awareness would be most beneficial, including groups that administer technology or handle sensitive information both inside and outside of IT (e.g., OT/SCADA, garages, vehicles) and organizational elements such as senior management, operations, safety, security, human resources, legal, and procurement/contracts. **Considerations and Guidelines:** • Review the agency's mission, vision, and strategic plan and understand how cybersecurity risk can disrupt the mission. Determine if major projects (e.g., system build out, renovation, integration with partners) are being undertaken in the next 1-5 years and to what extent they involve technology and influence cybersecurity risk. [APTA-SS-ECS-RP-004-23] • Tailor cybersecurity programs to support the organization's vision, mission, values, and requirements such that the program not only remains relevant but is aligned with organization-level priorities. [APTA-SS-ECS-RP-003-19] • Define organizational mission and business processes with consideration for information security and privacy and the resulting risk to organizational operations, organizational assets, individuals, and other organizations.	PM-11

NIST CSF 2.0 Subcategory	1. Protection and Management of Assets	2. Stakeholder Coordination	3. Organizational Development	Subcategory Rationale, Considerations, and Guidelines	Informative References
				• Envision cybersecurity as a contributor to concrete, visible, positive progress for the transit operator and its mission. [APTA-SS-ECS-RP-004-23]	
GV.OC-02: Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered	**E**	**E**	—	**1, 2**: A transit agency needs to document stakeholder needs and expectations for activities and concepts such as data protection, privacy, service availability, incident response, regulatory compliance, and communications during disruptions and should actively consider them when creating cybersecurity policies and practices. Stakeholders can include, among others, staff, management, contractors, service providers, the public, regulators, and emergency responders. By understanding what stakeholders expect, transit operators can prioritize cybersecurity efforts to ensure the protection of their most critical assets and services, such as operational control centers, fare systems, communications, and maintenance systems. **Considerations and Guidelines:** • Identify relevant external stakeholders and their cybersecurity-related expectations (e.g., privacy concerns of passengers/staff, business expectations of suppliers/vendors/partners, expectations of regulators and state and local agencies). • Use a tool like SIPOC (suppliers, inputs, processes, outputs and customers) for identifying stakeholders who contribute inputs to, or consume outputs of, a transit operation or business process/function. [APTA-SS-ECS-RP-004-23] • Meet with stakeholders to understand what motivates them, what they need from a cybersecurity program or security professional, what cybersecurity can contribute to them, and their relationship to others within the enterprise. [APTA-SS-ECS-RP-004-23]	PM-09
GV.RM-02: Risk appetite and risk tolerance statements are established,	**E**	—	—	**1:** To manage IT and OT risk strategically, risk appetite and tolerance statements are needed to communicate and establish the mitigations needed for protecting IT and OT assets and system operations. Risk appetite (i.e., statements about risk you can accept) and tolerance (i.e., statements about risk you cannot accept) will evolve as risks and threats evolve. This requires transit agencies to regularly review decisions	PM-09

NIST CSF 2.0 Subcategory	1. Protection and Management of Assets	2. Stakeholder Coordination	3. Organizational Development	Subcategory Rationale, Considerations, and Guidelines	Informative References
communicated, and maintained				about which protections, controls, or safeguards cannot be implemented, identify what risks remain that still need to be addressed to maintain the required operating conditions, and determine what protection mechanisms (compensating controls) can be implemented instead. **Considerations and Guidelines:** • Recognize, analyze and categorize a risk to determine its appropriate disposition (common dispositions include avoid, accept, monitor, transfer and mitigate) and identify response activities. [APTA-SS-CCS-RP-006-23] • Establish the organizational risk tolerance and communicate it throughout the organization, including guidance on how risk tolerance impacts ongoing decision-making activities. [APTA-SS-ECS-RP-001-14R1]	
GV.RM-05: Lines of communication across the organization are established for cybersecurity risks, including risks from suppliers and other third parties	—	E	E	**2, 3:** Defining and formalizing methods for communicating cyber risk across a transit agency, such as with management, IT/OT operations, legal, procurement, physical security, and HR, can help enable timely escalation and regular sharing of cybersecurity risk information, including risks from third parties and suppliers. **Considerations and Guidelines:** • Have a written plan that details who gets what cybersecurity risk information, how often, and in what format. Ensure information is appropriate for each group's needs and the sensitivity level of the information being shared. • Coordinate activities, to include information sharing, throughout the organization. [APTA-SS-ECS-RP-001-14R1] • Establish and maintain continuous collaboration between IT and OT teams to build relationships between different disciplines which will facilitate communication during cybersecurity incidents and emergency situations. [CISA-CPGs]	PM-09 PM-30 CISA CPG 1.A
GV.RR-01: Organizational	—	—	E	**3:** A single leader must be responsible and accountable for cybersecurity within a transit organization.	PM-02

NIST CSF 2.0 Subcategory	1. Protection and Management of Assets	2. Stakeholder Coordination	3. Organizational Development	Subcategory Rationale, Considerations, and Guidelines	Informative References
leadership is responsible and accountable for cybersecurity risk and fosters a culture that is risk-aware, ethical, and continually improving				**Considerations and Guidelines:** • Identify a named role/position/title as responsible and accountable for planning, resourcing, and executing cybersecurity activities. This role may handle activities such as managing cybersecurity operations at the senior level, requesting and securing budget resources, or leading strategy development to inform future positioning. • Ensure the most senior executive in the organization is accountable for identifying and neutralizing cybersecurity risks. Being accountable does not mean the executive does the work; the executive may appoint others who are responsible for doing the detailed work. The executive must hold relevant staff and contractors accountable on a regular basis to ensure that cybersecurity risks are routinely identified and addressed. [APTA-SS-ECS-RP-003-19]	
GV.RR-02: Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced	—	**E**	**E**	**2**: Identifying and understanding roles and responsibilities among stakeholders who may be responsible for certain aspects of the transit ecosystem such as specific IT systems, OT or field systems, networking equipment, workforce (e.g., contractors, vendors), or those that may have a role during an incident response or recovery process are critical to document and socialize. Memorandums of Understanding (MOUs) between operators and stakeholders will help document, communicate and enable these roles, responsibilities, and authorities. **3:** Workforce success depends on establishing, documenting, and enforcing cybersecurity roles, responsibilities, and authorities. This is often documented in a cybersecurity program plan or associated policies (e.g., account management plan, incident response plan, contingency plans). Personnel must know what's expected of them in their cybersecurity risk management roles, and the organization should have the mechanisms in place to communicate those expectations so they can be enforced.	PM-02 PM-13 PM-29

NIST CSF 2.0 Subcategory	1. Protection and Management of Assets	2. Stakeholder Coordination	3. Organizational Development	Subcategory Rationale, Considerations, and Guidelines	Informative References
				Considerations and Guidelines: • Appoint a senior information security officer (e.g., CISO) with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program. • Identify a named role/position/title as responsible and accountable for planning, resourcing, and execution of OT-specific cybersecurity activities. For small- and medium-sized transit agencies (SMTAs), this may be the same position as named in GV.RR-01. • Document authorities and decision-making responsibilities, ensuring that no conflicts of interest are created for individuals assigned multiple roles. This should be implemented by all transit organizations, especially SMTAs with staff who wear multiple hats. • Establish cybersecurity roles and responsibilities for the entire workforce, as well as third-party stakeholders (e.g., suppliers, customers, and partners). [APTA-SS-ECS-RP-001-14R1]	
GV.PO-01: Policy for managing cybersecurity risks is established based on organizational context, cybersecurity strategy, and priorities and is communicated and enforced	E	—	E	**1:** Cybersecurity risk management policies ensure consistency in how security measures are implemented across an organization. **3:** Strong, well-communicated cybersecurity policies promote a culture of security within the organization, encouraging employees to prioritize and take ownership of security in their daily activities. This cultural shift helps create a more resilient organization. **Considerations and Guidelines:** • Ensure cybersecurity policies are consistent with applicable laws, regulations, standards, and guidelines. For applicable transit operators, develop policies	AC-01 AT-01 AU-01 CM-01 CP-01 IR-01 MA-01 PE-01 PM-01 PT-01 RA-01 SA-01

NIST CSF 2.0 Subcategory	1. Protection and Management of Assets	2. Stakeholder Coordination	3. Organizational Development	Subcategory Rationale, Considerations, and Guidelines	Informative References
				related to handling Sensitive Security Information (SSI) with review by legal staff. [APTA-SS-ISS-RP-003-23] • Maintain an up-to-date Cybersecurity Incident Response Plan to quickly identify, isolate, and contain affected systems during a cybersecurity incident. [TSA-SD-1582-21-01C][3] • Maintain security policies (that address purpose, scope, roles, responsibilities, and management commitment and coordination among organizational entities), processes, and procedures that are used to manage the protection of information systems and assets. [APTA-SS-ECS-RP-001-14R1] • Communicate cybersecurity risk management policy and supporting processes and procedures across the organization.	
GV.SC-01: A cybersecurity supply chain risk management program, strategy, objectives, policies, and processes are established and agreed to by organizational stakeholders	—	E	—	**2:** Establishing a cyber supply chain risk management (C-SCRM) plan or strategy is essential to systematically identify, assess, communicate, and address risks associated with sensitive information and the use of various technologies and services in a transit organization. C-SCRM should take a comprehensive approach that considers supply chain risks to both technology-based inputs (e.g., software, hardware) and non-technology-based inputs (e.g., personnel, physical facilities). This process requires approval from key stakeholders, including those in charge of IT, OT, and safety-critical systems, to align the organization's broader cybersecurity strategies and objectives with risk management efforts across the transit ecosystem. A cybersecurity supply chain risk management plan involves a cross-functional team with representation from groups across the transit organization, including cybersecurity, IT, operations, legal, procurement/contracts, physical security, and safety.	PM-30 SR-02 SR-03

[3] While having an incident response plan is considered a cybersecurity best practice, it is important to recognize that not all organizations are bound by the TSA Security Directive (SD). This requirement applies specifically to certain transit agencies.

NIST CSF 2.0 Subcategory	1. Protection and Management of Assets	2. Stakeholder Coordination	3. Organizational Development	Subcategory Rationale, Considerations, and Guidelines	Informative References
				Considerations and Guidelines: • Develop a C-SCRM plan along with policies and procedures that guide implementation and improvement of the plan and the capability; socialize those policies and procedures with organizational stakeholders. [SP1305] • Establish a cross-organizational mechanism that ensures alignment between functions that contribute to C-SCRM management, such as IT, cybersecurity, legal, human resources, engineering, operations. [SP1305]	
GV.SC-02: Cybersecurity roles and responsibilities for suppliers, customers, and partners are established, communicated, and coordinated internally and externally	—	E	E	**2:** Transit operators are highly dependent on external service providers to help deliver and maintain critical technologies. Establishing and communicating clear and mutually acceptable requirements, plans, and procedures serves as protection for both the transit operator and their suppliers, customers, and partners. **3:** Transit staff with a mature level of cyber literacy will be necessary to identify, communicate and promote security needs and requirements in vendor discussions, requests for proposals, contracts, and service level agreements. **Considerations and Guidelines:** • Identify one or more specific roles or positions that will be responsible and accountable for planning, resourcing, and executing C-SCRM activities. [SP1305], [IR8276] • Establish a known set of security requirements or controls for all suppliers. Especially robust security requirements should be used for critical suppliers during procurement. [IR8276]	SR-02 SR-03
GV.SC-04: Suppliers are known and prioritized by criticality	E	E	—	**1, 2:** A necessary precursor to managing C-SCRM is knowing your organization’s technology suppliers and determining how critical each one is to your organization and its mission. Not all system components, functions, or services require the same level of protection. When considering the criticality of systems or their components, consider applicable laws, regulations, directives, policies, standards, system	RA-09 SR-06

NIST CSF 2.0 Subcategory	1. Protection and Management of Assets	2. Stakeholder Coordination	3. Organizational Development	Subcategory Rationale, Considerations, and Guidelines	Informative References
				functionality requirements, and system and component interfaces and dependencies. **Considerations and Guidelines:** - Develop criteria for supplier criticality based on, for example, the importance of the supplier's products or services to the agency's business, the sensitivity of data processed or stored by the supplier, and the degree of the supplier's access to the organization's systems. [SP1305] - Prioritize suppliers into criticality levels based on agency-specified criteria. See NIST IR 8179, *Criticality Analysis Process Model: Prioritizing Systems and Components* for more information on a structured method for prioritization. [IR8179] - Identify alternative sources of critical components to ensure uninterrupted production and delivery of products. [IR8276] - Keep a record of all suppliers, prioritized based on the criticality criteria. [SP1305]	
GV.SC-05: Requirements to address cybersecurity risks in supply chains are established, prioritized, and integrated into contracts and other types of agreements with suppliers and other relevant third parties	E	E	—	**1, 2:** Clearly defining cybersecurity requirements (e.g., software development attestations, secure remote access requirements, patching service level agreements (SLAs), vulnerability disclosure policies, incident notification timelines, right-to-audit, and end-of-life/end-of-support commitments) in contracts and agreements establishes accountability for suppliers and third parties. It ensures that they understand their responsibilities and are held to the same security standards as the transit operator. In defining requirements, encourage suppliers to prioritize cybersecurity in their own development and delivery processes, which can create a culture of security throughout the supply chain. **Considerations and Guidelines:** - Specify minimum cybersecurity requirements and response expectations in all vendor agreements. For SMTAs, see NIST's C-SCRM Quick Start Guide for how to use the CSF to define and communicate supplier requirements. [SP1305]	SA-04 SA-09 SR-06 SR-03 CISA CPG 1.D

NIST CSF 2.0 Subcategory	1. Protection and Management of Assets	2. Stakeholder Coordination	3. Organizational Development	Subcategory Rationale, Considerations, and Guidelines	Informative References
				• Involve staff with cybersecurity knowledge in developing rational and risk-informed cybersecurity requirements in contracts and SLAs. • Ensure that procurement documents and contracts, such as SLAs, stipulate that vendors and/or service providers notify the procuring customer of confirmed security vulnerabilities in their assets within a risk-informed time frame as determined by the organization. [CISA-CPGs]	
GV.SC-08: Relevant suppliers and other third parties are included in incident planning, response, and recovery activities	E	E	—	**1, 2:** Transit services are time-sensitive and critical to the daily lives of passengers. A cybersecurity incident, such as a ransomware attack or data breach, could disrupt operations, delay services, or compromise passenger safety. Suppliers and third parties often have specialized knowledge, tools, and resources to address incidents involving their systems or products. Including them in planning and response activities ensures a coordinated and rapid recovery, minimizing downtime and service disruptions. **Considerations and Guidelines:** • Include key suppliers in incident response, disaster recovery, and contingency plans and tests. [IR8276] • Ensure procurement documents and contracts, such as SLAs, stipulate that vendors and/or service providers notify the procuring customer of security incidents within a risk-informed time frame as determined by the organization. [CISA-CPGs]	CP-08 IR-01 SR-08 CISA CPG 1.D

5.2. Identify

Table 8. Subcategory-level Guidelines for the Identify Function

NIST CSF 2.0 Subcategory	1. Protection and Management of Assets	2. Stakeholder Coordination	3. Organizational Development	Subcategory Rationale, Considerations, and Guidelines	Informative References
ID.AM-01: Inventories of hardware managed by the organization are maintained	**E**	—	—	**1:** An up-to-date inventory of all hardware – including more difficult to inventory OT hardware such as wayside devices, onboard vehicle equipment (e.g., Automatic Vehicle Location systems, video surveillance systems, fare payment devices, and Wi-Fi routers), radio communication systems, and station infrastructure - is vital to ensure agencies know what equipment they have and what security measures are required. Well-designed inventory management also supports cybersecurity efforts, such as identifying and addressing security weaknesses, managing equipment configuration and lifecycles, and controlling device access. **Considerations and Guidelines:** • Maintain a regularly updated inventory of all organizational digital assets, including OT assets. Inventory should identify both the assets as well as their attributes, such as criticality, date of receipt, cost/contract number, model, serial number, manufacturer, supplier information, component type, and physical location. [CISA-CPGs] • Leverage NCCoE's SP 1800-23, *Energy Sector Asset Management* for an example implementation of and reference architecture for monitoring industrial control system assets in an OT network, including those located in remote sites. [SP1800-23]	CM-08 PM-05 CISA CPG 2.A
ID.AM-02: Inventories of software, services, and systems managed by the organization are maintained	**E**	—	—	**1:** Rationale for this Subcategory is similar to ID.AM-01 above. Maintaining inventories of software, services, and systems is vital to manage licensing, updates/patches, and vulnerabilities.	AC-20 CM-08 PM-05

NIST CSF 2.0 Subcategory	1. Protection and Management of Assets	2. Stakeholder Coordination	3. Organizational Development	Subcategory Rationale, Considerations, and Guidelines	Informative References
				Considerations and Guidelines: • Maintain inventories for all types of software, including commercial-off-the-shelf, open-source, and custom applications. Software details may include software name, version, vendor, deployment location (e.g., server, endpoint, controller), and licensing and expiration details.	
ID.AM-04: Inventories of services provided by suppliers are maintained	E	E	—	**1, 2**: Some transit operators rely on external services and vendors for both transportation services and general operations. An inventory of services, including cloud services, helps ensure that only authorized users and systems have access to specific services, reducing the risk of unauthorized access. In the event of a security breach, knowing which suppliers/services are in use and their associated data flows can help a transit agency respond quickly and effectively. **Considerations and Guidelines:** • Inventory and record the purpose and details of all external services used by the organization, including infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), and software-as-a-service (SaaS) offerings; APIs; and other application services. Where feasible, external information systems providing these services should be catalogued. Details can include service name, vendor, deployment location, and licensing and expiration details.	AC-20 SA-09 SR-02
ID.AM-05: Assets are prioritized based on classification, criticality, resources, and impact on the mission	E	—	—	**1:** Prioritizing assets based on classification, criticality, and the impact of their loss on mission execution is essential for effectively allocating security resources. Mission-critical systems, also called “crown jewels,” in transit can include operationally- and safety-critical systems such as computer-aided dispatch/automatic vehicle location assets, radio/LTE core network and software, fare payment gateways, train control interfaces, traction power/SCADA, depot charging/energy management, public information systems, and enterprise identity platforms. Asset prioritization also	RA-03 RA-09

NIST CSF 2.0 Subcategory	1. Protection and Management of Assets	2. Stakeholder Coordination	3. Organizational Development	Subcategory Rationale, Considerations, and Guidelines	Informative References
				supports risk-based decision making and resource allocation across the supply chain, while criticality helps inform contingency plans and disaster recovery plans. **Considerations and Guidelines:** • Leverage APTA's *Using Asset Criticality to Make More Informed Decisions in a Transit Agency* to provide guidance on how to perform a criticality analysis of assets and use this analysis for decision making. Asset criticality methods can be based on consequences of failure, risk of failure, and total cost of ownership. [APTA-SUDS-TAM-RP-010-21] • Estimate the degree of impact relative to each critical asset; the likelihood of an attack by a potential threat; and the likelihood that a specific vulnerability will be exploited. This can be based on factors such as prior history, attacks on similar assets, threat intelligence, warnings from law enforcement agencies, consultant advice, and the company's own judgment. [APTA-SS-CCS-RP-001-10]	
ID.AM-07: Inventories of data and corresponding metadata for designated data types are maintained	**E**	—	—	**1:** Cataloging and classifying all business data is an essential step in safeguarding data and ensuring compliance with relevant privacy regulations and security standards (e.g., PCI DSS). Identifying and categorizing data based on its sensitivity and importance will help a transit agency focus protection efforts where they are most needed. This approach ensures that highly sensitive information, such as personally identifiable information (PII), payment card information, or other security sensitive information, is secured with stricter controls, while less critical data is managed with proportionate measures. **Considerations and Guidelines:** • Identify and document the location of security sensitive information (e.g., PII, protected health information, or payment card data – some or all of which may reside in user account information) and the specific system components on which the information is processed and stored. Include data classification, ownership, access controls, and retention policies in the inventory.	CM-12

NIST CSF 2.0 Subcategory	1. Protection and Management of Assets	2. Stakeholder Coordination	3. Organizational Development	Subcategory Rationale, Considerations, and Guidelines	Informative References
ID.AM-08: Systems, hardware, software, services, and data are managed throughout their life cycles	E	—	—	**1**: Actively managing assets throughout their life cycle is essential to maintain security, performance, and compliance across the transit ecosystem. This supports risk management, operational efficiency, and the secure decommissioning of assets. Enterprise IT typically has established life cycle management processes that may need to be adjusted for OT systems, which have unique dependencies, vendors, and service contracts (e.g., warranties). As such, life cycle management processes for OT may differ from the organization's IT processes. Cloud services and virtualized assets may require separate life cycle management practices. **Considerations and Guidelines:** • Utilize the system development life cycle (SDLC) process to more efficiently manage IT systems. Utilize security activities outlined within each phase developed by NIST SP 800-100 to have a broad understanding of necessary security activities. [SP800-100], [APTA-SS-ECS-RP-001-14R1] • Regularly schedule, perform, document, and review maintenance and repair activities for all system components to ensure operational integrity and compliance.	MA-02 SA-03
ID.RA-01: Vulnerabilities in assets are identified, validated, and recorded	E	—	E	**1**: Identifying, validating, and recording vulnerabilities is crucial for effectively managing cybersecurity risks. This supports proactive risk mitigation, patch management, and secure supply chain practices. Since vulnerabilities can exist in any hardware, software, or service, identification and validation are key in prioritizing remediation. **3**: Frontline transit employees are the eyes and ears of every transit system. Bus and rail operators and maintenance employees, with the appropriate training, can be crucial in identifying and reporting unusual behavior or anomalies in vehicles, stations, and facilities that could indicate potential system vulnerabilities. Organizational development efforts (such as training, policy creation, and cross-team	CA-02 CA-07 CA-08 RA-03 RA-05 SI-04 SI-05 CISA CPG 2.C

NIST CSF 2.0 Subcategory	1. Protection and Management of Assets	2. Stakeholder Coordination	3. Organizational Development	Subcategory Rationale, Considerations, and Guidelines	Informative References
				collaboration) are essential to ensure vulnerabilities are effectively identified, validated, and recorded. The broader workforce is involved both directly (in technical roles) and indirectly (through awareness and reporting). **Considerations and Guidelines:** • Ensure all employees are trained in security awareness, behavioral awareness, and suspicious activity or potential vulnerability reporting. [APTA-SS-SRM-RP-005-12R1] • Conduct carefully planned activities (e.g., penetration testing in IT environments, vulnerability scanning) that support continuous monitoring and risk assessments of systems to identify, analyze, and validate potential vulnerabilities. • Monitor sources of cyber threat intelligence for information on new vulnerabilities in products and services. • Ensure that third parties with demonstrated expertise in (IT and/or OT) cybersecurity regularly validate the effectiveness and coverage of an organization's cybersecurity defenses. Validation exercises, which may include penetration tests, bug bounties, incident simulations, or table-top exercises, should include both unannounced and announced tests. [CISA-CPGs]	
ID.RA-05: Threats, vulnerabilities, likelihoods, and impacts are used to understand inherent risk and inform risk response prioritization	E	—	—	**1:** Realistic and actionable risk models depend on a thorough understanding of threats, vulnerabilities, likelihoods, and impacts to IT and OT assets and systems. Risk models built around this understanding ensure a complete view of the organization's risk posture and enable informed decision-making. **Considerations and Guidelines:** • Conduct risk assessments to understand the inherent risk present, determine the risk likelihood and magnitude of harm (including any adverse effects), and inform appropriate risk response options. Develop risk response options that enable the ability to address impacts appropriately. For more information on conducting	RA-03 RA-07

NIST CSF 2.0 Subcategory	1. Protection and Management of Assets	2. Stakeholder Coordination	3. Organizational Development	Subcategory Rationale, Considerations, and Guidelines	Informative References
				security risk assessments, see APTA SS-SIS-S-017-21, *Security Risk Assessment Methodology for Public Transit*. [APTA-SS-SIS-S-017-21] - Develop a threat and vulnerability assessment (TVA) as part of a Safety and Security Certification Verification Report (SSCVR). Incorporate physical and cybersecurity threat and vulnerability assessment mitigation measures into a systems' overall safety and security requirements. [APTA-SS-ISS-RP-008-24]	
ID.RA-07: Changes and exceptions are managed, assessed for risk impact, recorded, and tracked	E	—	—	**1:** Managing changes and exceptions is crucial for maintaining operational integrity and adapting to new requirements or technologies. To achieve this, processes for addressing vulnerabilities often use a risk-based approach that takes operational constraints into account—such as situations where patching OT devices is not feasible—which may, in turn, lead to delayed implementation or necessary trade-off decisions. **Considerations and Guidelines:** - Establish a configuration management control that includes a risk/impact analysis of proposed changes prior to implementation; explicit approval/disapproval prior to implementation; documentation and retention of records of all changes; and monitoring of the impacts of such changes. - Include OT security and safety personnel in change process management if the change to the system may impact safety or security. [SP800-82r3]	CM-03 CM-04
ID.RA-08: Processes for receiving, analyzing, and responding to vulnerability disclosures are established	E	E	—	**1:** Failure to effectively manage vulnerability disclosures can lead to a transit operator's noncompliance with legal obligations and regulatory requirements, jeopardize passenger safety, and undermine stakeholder trust. **2:** Establishing clear processes for vulnerability disclosures enables transit owners and operators to communicate with suppliers and customers, outline expectations for addressing vulnerabilities in contractual agreements, and define roles, responsibilities, and coordinated actions to address potential risks.	RA-05 RA-05(11) CISA CPG 2.D

NIST CSF 2.0 Subcategory	1. Protection and Management of Assets	2. Stakeholder Coordination	3. Organizational Development	Subcategory Rationale, Considerations, and Guidelines	Informative References
				Considerations and Guidelines: • Establish a process to monitor and scan for vulnerabilities. The process should include a method for sharing information and results from the scans, as well as a notification process with stakeholders so that awareness and remediation (as appropriate) can occur. • Maintain a public, easily discoverable method for security researchers to notify (e.g., via email address or web form) a transit agency of vulnerable, misconfigured, or otherwise exploitable assets. [CISA-CPGs]	
ID.RA-10: Critical suppliers are assessed prior to acquisition	E	E	—	**1, 2**: By assessing critical suppliers for cybersecurity and supply chain risk prior to acquisition, a transit operator can proactively identify and mitigate threats to OT and IT systems - such as signaling systems, dispatch systems, communications, fare collection systems, vehicle onboard systems, and operations control centers. This ensures that suppliers align with transit-specific security and compliance requirements and protect their operations and data. This is a fundamental part of a robust supply chain risk management strategy and helps the operator maintain a strong cybersecurity posture. **Considerations and Guidelines:** • Review suppliers to identify potential supply-chain-related risks. • Understand associated security impacts when integrating legacy and newer assets and systems or modernizing IT/OT. [APTA-SS-CCS-RP-006-23]	SR-06
ID.IM-02: Improvements are identified from security tests and exercises, including those done in coordination with suppliers and relevant third parties	E	E	—	**1, 2**: Engaging both internal and external stakeholders—such as operations control center staff, maintenance teams, fare collection and IT systems personnel, and contractors—in security tests and exercises to identify potential incident response strategies and areas for improvement in advance. Involving all relevant parties in this process helps uncover necessary updates to policies, processes, and procedures, ultimately enhancing overall operational effectiveness. These exercises evaluate not only the capability and impact of external adversaries attempting to breach the network but also the potential actions of internal threats or an "assume breach"	CA-02 CA-05 CP-01 CP-02 IR-01 IR-04 IR-08 RA-03

NIST CSF 2.0 Subcategory	1. Protection and Management of Assets	2. Stakeholder Coordination	3. Organizational Development	Subcategory Rationale, Considerations, and Guidelines	Informative References
				scenario. Evaluation identifies improvement opportunities, and improvement planning provides a disciplined process for implementing corrective actions. **Considerations and Guidelines:** • Conduct tabletop exercises with key stakeholders. Organize tabletop exercises with staff involved in incident response to simulate different cyberattack scenarios, helping everyone understand roles and improve response coordination. Ensure that any third-party cybersecurity or IT service providers, as well as OT suppliers/vendors, are included in tabletop exercises and are aware of the business's SLA expectations. • Prepare, maintain, update, and regularly drill IT and OT cybersecurity incident response plans for both common and organizationally-specific (e.g., locality) threat scenarios and tactics, techniques, and procedures (TTPs). When conducted, tests or drills are as realistic as feasible. Incident response plans are drilled at least annually and are updated within a risk-informed time frame following the lessons learned portion of any exercise or drill. [CISA-CPGs] • Consider leveraging the Integrated Preparedness Plan process to develop planning, training, and exercise cycles. Refer to APTA SS-SEM-S-004-09, Rev. 2, *Transit Exercises* for minimum practices for conducting transit exercises, including cybersecurity exercises. [APTA-SS-SEM-S-004-09R2]	RA-05 RA-07 SI-02 SI-04 CISA CPG 1.C
ID.IM-04: Incident response plans and other cybersecurity plans that affect operations are established, communicated, maintained, and improved	E	E	—	**1, 2**: Establishing and maintaining incident response and other cybersecurity plans (e.g., contingency plans, vulnerability management plans) supports a transit agency's mission and operation. While the robustness of implementing these plans will vary, these plans establish direction and guidance to transit agencies, enable proactive responses, and improve resilience to cyberthreats.	CP-02 IR-08 PL-02 SR-02

NIST CSF 2.0 Subcategory	1. Protection and Management of Assets	2. Stakeholder Coordination	3. Organizational Development	Subcategory Rationale, Considerations, and Guidelines	Informative References
				Considerations and Guidelines: • Incorporate lessons learned into plans as part of achieving overall continuity of mission and business functions. Plans may include contingency, incident response, and system security plans. • Develop and maintain a current Cybersecurity Incident Response Plan to address potential cybersecurity incidents affecting rail systems or facilities, minimizing the risk of operational disruptions and other significant impacts on critical business functions. [TSA-SD-1582-21-01C][4] • Consider developing ICS-aligned cyber incident playbooks that integrate IT, OT, operations, and external parties (e.g., TSA, FTA, local emergency management).	

[4] While having an incident response plan is considered a cybersecurity best practice, it is important to recognize that not all organizations are bound by the TSA Security Directive (SD). This requirement applies specifically to certain transit agencies.

535
5.3. Protect

536 **Table 9. Subcategory-level Guidelines for the Protect Function**

NIST CSF 2.0 Subcategory	1. Protection and Management of Assets	2. Stakeholder Coordination	3. Organizational Development	Subcategory Rationale, Considerations, and Guidelines	Informative Reference
PR.AA-01: Identities and credentials for authorized users, services, and hardware are managed by the organization	**E**	—	—	**1**: Implementing robust identity and access management practices allows a transit agency to safeguard sensitive information and critical systems, such as wayside and station monitoring and management (OT) equipment, by ensuring that only authenticated and authorized entities have access. These practices should also extend to vendor and third-party user accounts. **Considerations and Guidelines:** • Carefully manage administrator, shared, and vendor accounts for support through established processes to mitigate risks. Restrict use of shared accounts, when possible. • Provision unique and separate credentials for similar services and asset access on IT and OT networks. [CISA-CPGs] • Store credentials securely using a credential/password manager, vault, or other privileged account management solution. [CISA-CPGs] • Ensure users do not (or cannot) reuse passwords for accounts, applications, services, etc. [CISA-CPGs] • Assign service account/machine account passwords that are unique from all member user accounts. [CISA-CPGs] • Physically label authorized hardware with an identifier for inventory and servicing purposes. [IR8183r2]	AC-01 AC-02 AC-14 IA-02 IA-03 IA-04 IA-05 CISA CPG 3.C 3.D 3.K
PR.AA-03: Users, services, and hardware are authenticated	**E**	—	—	**1**: Many OT systems continue to rely on default passwords, lack robust credential management systems, and fail to implement policies for deleting old accounts, enforcing password changes, or ensuring password complexity. These gaps can significantly increase the risk of unauthorized access, compromising the security of critical operational systems.	AC-07 AC-12 CISA CPG 3.A

NIST CSF 2.0 Subcategory	1. Protection and Management of Assets	2. Stakeholder Coordination	3. Organizational Development	Subcategory Rationale, Considerations, and Guidelines	Informative Reference
				Considerations and Guidelines: • Use MFA for all IT accounts and remote access services, prioritizing high-risk and privileged accounts. [CISA-CPGs] • Change default passwords for all hardware, software, and firmware before network connection, including IT assets for OT systems such as administration web pages. If default passwords cannot be changed, document and monitor compensating controls for network and login activity. [CISA-CPGs] • Require strong passwords for all password-protected IT and OT assets, when technically feasible; use passphrases and password managers, and apply compensating controls with logging, if needed. [CISA-CPGs] • Limit failed login attempts and take action when limits are reached. [CISA-CPGs] • Implement additional physical access controls and auditing measures to track access and activity on systems when OT systems cannot accommodate modern authentication mechanisms. [SP800-82r3] • Use shared accounts with caution. If shared accounts are necessary, ensure their use is tightly controlled and monitored. [SP800-82r3] • Ensure that authorized personnel can access accounts for safety systems under emergency conditions. [SP800-82r3]	3.B 3.E 3.F
PR.AA-05: Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties	E	—	—	**1:** Managing access permissions by adhering to the principles of least privilege and separation of duties is a foundational cybersecurity best practice for protecting sensitive data and systems. However, safety must remain a priority when implementing these solutions. Access control mechanisms must be designed to minimize latency or operational delays that could impact the real-time functionality of OT devices and safety-critical operations. **Considerations and Guidelines:** • Restrict access and privileges to the minimum necessary. [CISA-CPGs]	AC-01 AC-02 AC-03 AC-05 AC-06 CISA CPG 3.D 3.G 3.H

NIST CSF 2.0 Subcategory	1. Protection and Management of Assets	2. Stakeholder Coordination	3. Organizational Development	Subcategory Rationale, Considerations, and Guidelines	Informative Reference
				• Require administrators to use separate accounts for non-administrative tasks (e.g., for business email, web browsing) and reevaluate privileges regularly to validate the need for elevated privileges. [CISA-CPGs] • Identify and document actions that can be performed on critical systems without identification or authentication (e.g., emergency stop). • Review logical and physical access privileges periodically and whenever someone changes roles or leaves the organization, or when a contract is expired/terminated; promptly rescind privileges that are no longer needed. [CISA-CPGs] • Scan for rogue wired or wireless devices attached to control/communications networks every other month or on a frequency informed by a risk assessment. [APTA-SS-CCS-RP-004-16] • Define and document usage restrictions, configuration and connection requirements, and implementation guidelines for each permitted type of remote access. Ensure that each type of remote access is authorized before enabling connection to the system.	
PR.AA-06: Physical access to assets is managed, monitored, and enforced commensurate with risk	E	—	—	**1:** Physical security is a critical component of a comprehensive cybersecurity strategy for transit agencies. Cyberattacks on OT systems can begin with physical access, such as plugging unauthorized devices into network ports or tampering with hardware. Many OT assets in the transit sector, such as trackside equipment, substations, and communication towers, are in remote or distributed areas. These assets are particularly vulnerable to theft, vandalism, or tampering. By securing physical access points, transit agencies can reduce the risk of cyber-physical attacks and protect safety-critical systems and sensitive data.	PE-02 PE-03 PE-06 PE-08 PE-20

NIST CSF 2.0 Subcategory	1. Protection and Management of Assets	2. Stakeholder Coordination	3. Organizational Development	Subcategory Rationale, Considerations, and Guidelines	Informative Reference
				Considerations and Guidelines: • Deploy physical monitoring systems (e.g., cameras, sensors, and identification systems) to monitor facilities and restrict access. [SP800-82r3] • House operational and safety-critical electronic equipment in a six-sided physical enclosure with two-factor authentication to access and warn on unauthorized physical access. [APTA-SS-CCS-RP-002-13], [APTA SS-CCS-RP-004-16] • Lock equipment cabinets when not needed for operation or safety; set OT asset keys of devices (e.g., programmable logic controllers (PLCs), safety systems) to the "RUN" position unless otherwise specified. [SP800-82r3] • Implement a key management system to manage and secure physical keys. [SP800-82r3] • Extend physical access control beyond physical hardware storage to include the location of communication transmission wires, electric power sources, HVAC systems, and other resources linked to IT infrastructure. [APTA-SS-ECS-RP-001-14R1] • Assess the security controls at remote locations and analyze their potential impact on the overall system, with a focus on how weaker security at these sites could influence the broader network. Use this evaluation to prioritize the implementation of additional or enhanced controls based on risk. [SP800-82r3] • Consider environmental, legal, and regulatory factors when designing physical access controls. [SP800-82r3]	
PR.AT-01: Personnel are provided with awareness and training so that they possess the knowledge and skills to perform general tasks with security risks in mind	—	—	**E**	**3:** Consistent and targeted training for all staff, including frontline workers—drivers, dispatchers, and technicians—plays a critical role in fostering efficiency and safety across operations. **Considerations and Guidelines:** • Provide initial cybersecurity training for new employees prior to accessing systems. [CISA-CPGs]	AT-02 AT-03 CISA CPG 3.J

NIST CSF 2.0 Subcategory	1. Protection and Management of Assets	2. Stakeholder Coordination	3. Organizational Development	Subcategory Rationale, Considerations, and Guidelines	Informative Reference
				• Conduct at least annual training for all organizational employees and contractors in recognizing social engineering attempts and other common attacks, reporting suspicious activity, complying with acceptable use policy, and performing basic cyber hygiene tasks such as selecting and protecting passwords. [CISA-CPGs]	
PR.AT-02: Individuals in specialized roles are provided with awareness and training so that they possess the knowledge and skills to perform relevant tasks with security risks in mind	E	E	E	**1, 2, 3**: Provide additional training for individuals with specialized roles in operating buses and rail systems and incident response, as well as for those in leadership positions, to prepare them for responding appropriately in both normal and adverse operating situations. Emphasize training as essential for delivering services and maintaining safe operations. **Considerations and Guidelines:** • Create a training program for employees, vendors and partners around transit agency control and communications security. [APTA-SS-CCS-RP-004-16] • Provide adequate training for employees in security-sensitive positions to identify and respond to potential threats. [49-CFR-1582.113] • Implement training programs for software developers to recognize coding flaws, incorporating the NIST Secure Software Development Framework (SSDF) to guide secure coding practices; ensure software development management provides secure coding training and uses testing tools, techniques, and industry best practices, such as DevSecOps, to identify and address flaws in software. [APTA-SS-CCS-RP-004-16] • Conduct OT-specific cybersecurity training for personnel who maintain or secure OT as part of their regular duties, in addition to basic cybersecurity training, on at least an annual basis. [CISA-CPGs]	AT-03 CISA CPG 3.J
PR.DS-01: The confidentiality, integrity, and availability of data-at-rest are protected	E	E	—	**1, 2**: Proper protection of sensitive data at rest, such as through encryption and secure backups, ensures that critical information can be restored quickly in the event of a cyberattack, hardware failure, or other incident. When using third-party services, transit agencies should also verify that providers implement robust data protection	CA-03 CP-09 SC-07 SC-13 SC-28

NIST CSF 2.0 Subcategory	1. Protection and Management of Assets	2. Stakeholder Coordination	3. Organizational Development	Subcategory Rationale, Considerations, and Guidelines	Informative Reference
				measures, including encryption, secure backup procedures, and clear recovery processes, to safeguard sensitive information and maintain operational continuity. **Considerations and Guidelines:** • Use encryption, digital signatures, and cryptographic hashes to protect the confidentiality and integrity of stored data in files, databases, virtual machine disk images, container images, and other resources. • Prohibit the storage of sensitive data, including credentials, in plaintext across the organization, and ensure access is restricted to authenticated and authorized users. [CISA-CPGs] • Protect and control portable storage devices containing sensitive transit agency data-at-rest while in storage. • Perform a risk analysis to determine how data-at-rest is protected by vendor or third-party service providers and whether additional protections should be implemented.	CISA CPG 3.K
PR.DS-02: The confidentiality, integrity, and availability of data-in-transit are protected	**E**	—	—	**1:** Implementing and configuring encryption in transit is critical to protecting the data of the agency and its users. **Considerations and Guidelines:** • Monitor transit systems at the external boundary and at key internal points to detect unauthorized information flows. • Use SSL/TLS to protect data in transit when feasible. [CISA-CPGs] • Identify and replace weak or outdated encryption with strong algorithms; prepare for post-quantum cryptography. [CISA-CPGs] • Encrypt OT communications, especially for remote or external connections, and where latency issues would not impact operations. [CISA-CPGs]	CA-03 SC-07 SC-11 SC-13 CISA CPG 3.K

NIST CSF 2.0 Subcategory	1. Protection and Management of Assets	2. Stakeholder Coordination	3. Organizational Development	Subcategory Rationale, Considerations, and Guidelines	Informative Reference
PR.DS-11: Backups of data are created, protected, maintained, and tested	E	—	—	**1**: Regularly backing up operational systems and tracking the physical location of backups are essential for ensuring rapid recovery from cyber incidents, hardware failures, or data loss. **Considerations and Guidelines:** • Back up all operational systems regularly based on a risk assessment, but no less than annually. [CISA-CPGs] • Maintain a list of system backups, test them for reliability and integrity, and store backup procedures separately in a centralized location. [SP800-82r3] • Track the physical location of backups. [SP800-82r3] • Store backups separately from source systems, test procedures for restoring from backup annually, and include documentation on OT assets including configurations, roles, PLC logic, engineering drawings, and tools. [CISA-CPGs]	CP-06 CP-09 CISA CPG 3.0
PR.PS-01: Configuration management practices are established and applied	E	—	—	**1**: Proper configuration management helps maintain up-to-date software and hardware, reducing the risk of vulnerabilities caused by outdated or misconfigured systems. Change management in both IT and OT must consider their impacts on each other, especially at points of integration and where shared services exist. Configuration management oversight extends to ensuring visibility into change orders, as even seemingly innocuous changes to networks can have significant consequences across both environments. By standardizing and monitoring configurations, transit agencies can enhance system integrity, streamline maintenance, support compliance with regulatory standards, and protect the infrastructure that underpins daily operations. **Considerations and Guidelines:** • Document baseline and current configurations for all critical IT and OT assets to improve vulnerability management, response, and recovery. Perform and track	CM-01 CM-02 CM-03 CM-04 CM-05 CM-09 CISA CPG 3.N

NIST CSF 2.0 Subcategory	1. Protection and Management of Assets	2. Stakeholder Coordination	3. Organizational Development	Subcategory Rationale, Considerations, and Guidelines	Informative Reference
				periodic reviews and updates. Retain previous versions of the baseline configuration to support rollback. [CISA-CPGs], [APTA-SS-CCS-RP-004-16] • Use a centralized or distributed configuration management system, whether manual or software-based, to manage software, executables, and configuration files for each safety- and operationally-critical device. [APTA-SS-CCS-RP-004-16] • Configure systems to provide only required capabilities. Review the baseline configuration and disable unused capabilities. Conduct security impact assessments in connection with change control reviews.	
PR.PS-02: Software is maintained, replaced, and removed commensurate with risk	E	—	—	**1**: Proper maintenance of software through patching, removal, or replacement ensures that systems remain functional, secure, and up to date. A transit agency should be able to confirm the integrity of files on each PLC or controller in safety-critical systems. **Considerations and Guidelines:** • Require approval for installing or deploying new software/software versions; maintain a risk-informed allowlist of approved items. [CISA-CPGs] • Test patches in OT environments before deployment, establish recovery plans, and schedule updates during maintenance windows. [SP800-82r3] • Apply compensating controls, such as network isolation and physical access restrictions, for OT systems with unsupported software that cannot be patched or updated. [SP800-82r3] • Verify host file integrity using cryptographic checksums on safety-critical controllers, such as vital PLCs, except where large or complex file structures make this impractical. [APTA-SS-CCS-RP-002-13] • Limit remote vendor access to temporary, security-controlled sessions for installation or maintenance tasks. [SP800-82r3]	CM-11 SI-02 SI-07 CISA CPG 3.P
PR.PS-03: Hardware is maintained, replaced, and	E	—	—	**1**: By prioritizing hardware maintenance actions according to risk, a transit agency can address vulnerabilities proactively, minimize the likelihood of failures or security	CM-07(09) SC-49

NIST CSF 2.0 Subcategory	1. Protection and Management of Assets	2. Stakeholder Coordination	3. Organizational Development	Subcategory Rationale, Considerations, and Guidelines	Informative Reference
removed commensurate with risk				breaches, and optimize resource allocation. This approach helps prevent the continued use of unsupported or obsolete devices, reduces exposure to cyber and operational risks, and supports the overall safety and integrity of critical infrastructure. **Considerations and Guidelines:** • Require approval for installation or deployment of new hardware or firmware, maintain a risk-informed allowlist of approved assets and versions, and align OT asset changes with defined change control and testing activities. [CISA-CPGs] • Inspect maintenance tools brought into the agency (e.g., diagnostic test equipment, network taps, and laptops). Scan maintenance tools and portable storage devices for malicious code before they are used on transit systems. • Disable or secure any unnecessary USB ports or other entry ports on safety-critical devices and equipment, as well as on publicly accessible systems such as ticketing machines, passenger information displays, and other vehicle, station, or track-based equipment. [APTA-SS-CCS-RP-002-13] • Document device maintenance and related issues, record hardware no longer maintained or manufactured, and develop end-of-life plans for unsupported devices. [SP800-82r3] • Implement an asset disposal program that includes wiping or destroying critical information or media before disposing of information-bearing assets. [SP800-82r3]	SC-51 CISA CPG 3.P
PR.PS-04: Log records are generated and made available for continuous monitoring	E	—	—	**1:** Audit logs enable accountability and support forensic investigations by showing when cybersecurity measures were active and when issues occurred. Regular analysis of logs helps identify unexpected conditions.	AU-02 AU-03 AU-11 AU-12 CISA CPG 3.Q

NIST CSF 2.0 Subcategory	1. Protection and Management of Assets	2. Stakeholder Coordination	3. Organizational Development	Subcategory Rationale, Considerations, and Guidelines	Informative Reference
				Considerations and Guidelines: • Collect and store access- and security-focused logs for detection and incident response; notify security teams when critical log sources are disabled. [CISA-CPGs] • Collect network traffic and communications for OT assets lacking standard logs. [CISA-CPGs] • Compare and synchronize the internal system clocks to an authoritative time source (e.g., NTP server, radio clock, GPS) to maintain consistent timestamps across all systems. • Store logs in a central system accessible only to authorized, authenticated users, and retain logs for a duration based on risk or regulatory requirements. [CISA-CPGs]	
PR.IR-01: Networks and environments are protected from unauthorized logical access and usage	E	—	—	**1**: Transit agency cybersecurity and safety engineers should work together to document and justify that network protections do not adversely affect the functional safety or certified operation of the system. This can help avoid triggering recertification by demonstrating that changes are isolated and non-intrusive. **Considerations and Guidelines:** • Configure applications and external network connections to block unauthorized access by using firewalls, closing unnecessary ports, enforcing authentication, using encrypted connections like SSL, monitoring data exchange, and incorporating network segmentation where appropriate. [APTA-SS-ECS-RP-001-14R1] • Deny all connections to the OT network by default unless explicitly allowed for specific system functionality and ensure necessary communications between IT and OT networks pass through monitored intermediaries such as firewalls, bastion hosts, jump boxes, or demilitarized zones (DMZs) that capture network logs and only allow connections from approved assets. [CISA-CPGs]	AC-03 SC-07 CISA CPG 3.I 3.S

NIST CSF 2.0 Subcategory	1. Protection and Management of Assets	2. Stakeholder Coordination	3. Organizational Development	Subcategory Rationale, Considerations, and Guidelines	Informative Reference
				• Enforce OT network isolation using unidirectional gateways, such as data diodes, to minimize exposure when transferring data to the corporate network, ensuring no remote access is required. [SP800-82r3]	
PR.IR-02: The organization's technology assets are protected from environmental threats	E	—	—	**1:** Physical risks such as fires, failures in heating and air conditioning systems, flooding, and other natural disasters may cause service interruption and damage equipment or data. **Considerations and Guidelines:** • Implement and enforce policies and regulations regarding environment protection systems (e.g., emergency and safety systems, fire protection systems, and environment controls) for transit systems. Protections should be implemented in consideration of the risks and relative impacts to transit agency IT and OT systems. • Include considerations for local environmental threats, such as floods, fire, wind, and excessive heat and humidity, in site-specific evaluations. [SP800-82r3], [APTA-SS-ECS-RP-001-14R1]	CP-02 PE-09 PE-10 PE-11 PE-12 PE-13 PE-14 PE-15 PE-18
PR.IR-03: Mechanisms are implemented to achieve resilience requirements in normal and adverse situations	**E**	—	—	**1**: Identifying and mitigating critical risks, including single points of failure, in transit systems is essential for maintaining availability, data integrity, security, and operational resilience. Employing redundancy, decentralization, regular testing, and robust security measures help minimize vulnerabilities, ensure continued service, and rapid recovery from failures. Resiliency measures should be clearly defined in contracts, along with an understanding of how other entities in an agency's supply chain address adverse situations. Ensuring the availability of transit services is a top priority, and it is essential to incorporate resilience mechanisms, such as including backup suppliers or alternative sourcing agreements in contracts, into supply chain management for this sector.	CP family IR family SC-39

NIST CSF 2.0 Subcategory	1. Protection and Management of Assets	2. Stakeholder Coordination	3. Organizational Development	Subcategory Rationale, Considerations, and Guidelines	Informative Reference
				Considerations and Guidelines: • Develop contingency plans to identify alternative locations for business operations and information security in the event that buildings are compromised. [APTA-SS-ECS-RP-001-14R1] • Identify and implement redundancies to ensure uninterrupted service. [APTA-SS-ECS-RP-001-14R1]	

5.4. Detect

Table 10. Subcategory-level Guidelines for the Detect Function

NIST CSF 2.0 Subcategory	1. Protection and Management of Assets	2. Stakeholder Coordination	3. Organizational Development	Subcategory Rationale, Considerations, and Guidelines	Informative Reference
DE.CM-01: Networks and network services are monitored to find potentially adverse events	E	—	—	**1:** A transit operator should be able to monitor IT and OT networks, systems, and services. Operators should seek to enable detection and alerting of anomalous activities and events or unusual activity where technically feasible, while planning and building the capability to do so across legacy systems and infrastructure, as needed. **Considerations and Guidelines:** • Develop and implement access management, configuration management, and continuous monitoring strategies and practices to enable transit agencies to safeguard transit systems and networks; have practices and procedures in place to detect potentially adverse events. • Include wired and wireless networks, network communications and flows, network services (e.g., DNS and BGP), and the presence of unauthorized or rogue networks in system monitoring practices. [SP800-61r3] • Ensure OT cybersecurity personnel are part of the diagnostic process of interpreting alerts provided by network monitoring tools. [SP800-82r3] • Subject system use monitoring solutions and sensors to extensive testing and implementation in a test environment before deploying to devices in the OT system. [SP800-82r3] • Improve incident detection using enterprise incident management systems as part of a holistic approach to incident response. [APTA-SS-ECS-RP-001-14R1]	AC-02 CA-07 CM-03 SI-04
DE.CM-02: The physical environment is monitored to find potentially adverse events	E	—	—	**1:** Transit assets are highly accessible to the public, which can increase the risk of adverse events affecting transit IT, OT, and data. As a result, it is essential to implement monitoring tools and techniques within the physical environment to protect transit assets and identify potential adverse events as part of an effective incident response strategy.	CA-07 PE-03 PE-06

NIST CSF 2.0 Subcategory	1. Protection and Management of Assets	2. Stakeholder Coordination	3. Organizational Development	Subcategory Rationale, Considerations, and Guidelines	Informative Reference
				Considerations and Guidelines: • Implement monitoring capabilities, such as video surveillance systems (VSS), closed-circuit television (CCTV), and intrusion detection systems (IDS) that can detect and alert transit agencies to potential threats and physical attacks to transit assets. [APTA-SS-SIS-S-010-13R1] • Monitor physical environments, including all successful and failed access attempts into all controlled areas, the movement of people and equipment into and out of secure areas of facilities, and signs of tampering with physical access controls. [SP800-61r3] • Develop and implement continuous monitoring strategies and practices that enable transit agencies to execute monitoring activities for physical environments and assets in those environments. This includes monitoring and implementing physical access controls to prevent access to non-public areas and assets. • Implement layers of physical security for transit assets (e.g., camera pointed toward electronic equipment cabinets in buses to monitor and record unauthorized access attempts). [APTA-SS-CCS-WP-005-19] • Establish physical presence and patrols at critical infrastructure locations in addition to cybersecurity measures. [APTA-SS-ISS-RP-007-24]	
DE.CM-06: External service provider activities and services are monitored to find potentially adverse events	E	E	—	**1:** Transit operators that depend on external service providers require robust systems to protect, detect, and contain malicious or suspicious events that could put a transit operator and its assets at risk. Real-time visibility enables early identification of threats, making detection capabilities essential for ensuring the safety and security of assets from both cyber and operational standpoints. **2:** External service providers—such as vendors, supply chain partners, and managed security service providers (MSSPs)—often exercise significant control over the security of the activities or services they deliver, including OT, cloud solutions, threat detection, and subscribed systems. Consequently, the ability to detect potentially	CA-07 SA-04 SA-09 SI-04

NIST CSF 2.0 Subcategory	1. Protection and Management of Assets	2. Stakeholder Coordination	3. Organizational Development	Subcategory Rationale, Considerations, and Guidelines	Informative Reference
				adverse events depends on these providers implementing effective monitoring tools, techniques, and capabilities to identify deviations from expected behaviors. Transit agencies may formalize their monitoring expectations through documentation such as contracts or MOUs and may require enhanced communication protocols when potential events are detected. **Considerations and Guidelines:** • Conduct ongoing security monitoring of external service providers' remote and onsite activities on transit systems (e.g., unauthorized external personnel, activities, connections, devices, access points, software). • Monitor activity from cloud-based services, internet service providers, and other service providers for deviations from expected behavior. [SP800-61r3] • Establish procedures and processes to meet the security requirements expected of external service providers, enabling effective detection of potential adverse events. [APTA-SS-ECS-RP-001-14R1]	
DE.CM-09: Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events	**E**	—	—	**1:** Similar to Subcategories DE.CM-01 and DE.CM-06. Hardware, software, runtime environments, and their data are critical to transit agencies' infrastructure and enterprise information systems. **Considerations and Guidelines:** • Establish configuration settings to keep track of hardware, software, and runtime environments, as well as important data, to help identify potential issues. Monitoring activities may include regularly checking for unauthorized software installations, reviewing user access logs for unusual authentication attempts, and keeping an eye on email and file sharing services for signs of malware or data leaks. [SP800-61r3], [APTA-SS-SIS-S-010-13R1] • Periodically compare systems to known good configurations to spot any unexpected changes that might indicate tampering or compromise. [SP800-61r3], [APTA-SS-ECS-RP-001-14R1]	CA-07 CM-06 CM-11 SI-04

NIST CSF 2.0 Subcategory	1. Protection and Management of Assets	2. Stakeholder Coordination	3. Organizational Development	Subcategory Rationale, Considerations, and Guidelines	Informative Reference
DE.AE-02: Potentially adverse events are analyzed to better understand associated activities	E	—	—	**1:** Analyzing potentially adverse events (e.g., multiple failed login attempts, unplanned shutdowns, unusually heavy network traffic, unauthorized communication to external IPs) enables transit agencies to determine whether an incident is genuine or a false positive, and to take the necessary actions to protect assets and maintain uninterrupted or minimally disrupted services. Automated tools, such as security information and event management (SIEM) and security orchestration automation and response (SOAR) systems, can accelerate the monitoring and identification of events that warrant further examination by staff. **Considerations and Guidelines:** • Review audit records (e.g., logs), which may provide further insight into suspicious activity or a potential threat that requires further investigation. [APTA-SS-CCS-RP-006-23]. Use of automated tools can improve detection accuracy and provide details related to a threat actor. Manually review log events where automation is not appropriate. [SP800-61r3], [APTA-SS-CCS-RP-006-23] • Conduct analysis combined with other data points to process potential threat activities and disseminate information to appropriate recipients. [APTA-SS-CCS-RP-006-23] • For SMTAs: Consider partnering with an MSSP to provide monitoring and response capabilities; leveraging cloud-native tools and/or open-source security tools that offer basic automation and monitoring features; and collaborating with other local organizations and industry groups (e.g., ISACs) to share resources, threat intelligence, and best practices.	AU-06 CA-07 IR-04 SI-04
DE.AE-06: Information on adverse events is provided to authorized staff and tools	E	E	—	**1, 2:** Comparable to Subcategory DE.AE-02, once an adverse event is confirmed, relevant information should be shared with authorized personnel and systems to support recommendations for appropriate actions. By combining automated tools for rapid information correlation with human expertise and analysis, a transit agency can respond swiftly and make informed, risk-based decisions to safeguard assets,	PM-16

NIST CSF 2.0 Subcategory	1. Protection and Management of Assets	2. Stakeholder Coordination	3. Organizational Development	Subcategory Rationale, Considerations, and Guidelines	Informative Reference
				maintain service continuity, and communicate promptly with both internal and external stakeholders. **Considerations and Guidelines:** • Coordinate with personnel and provide the appropriate tools for them to respond and provide operations within the context of adverse events and elevated threats. [APTA-SS-ISS-RP-007-24] • Implement automated anomaly detection through use of tools (e.g., SOAR) that can support a 360-degree perspective of an incident. Provide information to appropriate staff (e.g., analysts) for evidence-gathering, investigation, and recommendations on the best course of action. [APTA-SS-CCS-RP-006-23] • Designate a Cybersecurity Coordinator (and alternate, if appropriate) to work with appropriate law enforcement and emergency response agencies to manage security incidents. [TSA-SD-1582-21-01C] [5]	

[5] It is important to note that not all organizations are bound by the TSA Security Directive (SD). This requirement applies specifically to certain transit agencies.

5.5. Respond

Table 11. Subcategory-level Guidelines for the Respond Function

NIST CSF 2.0 Subcategory	1. Protection and Management of Assets	2. Stakeholder Coordination	3. Organizational Development	Subcategory Rationale, Considerations, and Guidelines	Informative References
RS.MA-01: The incident response plan is executed in coordination with relevant third parties once an incident is declared	E	E	E	**1, 2, 3:** Transit agencies should be prepared to manage incidents quickly to protect service delivery and sensitive data. They may coordinate response efforts across different teams or asset types (IT and OT) for consistency. Effective incident response requires clear documentation and communication among stakeholders, including event confirmation, notifications, and alerts. Plans should also address supply chain disruptions. **Considerations and Guidelines:** • Establish formal agreements and communication channels with third parties (e.g., local police/fire/EMS, external vendors, digital forensic services) in advance of a security incident to enable rapid and effective incident response. • For OT environments: Work with external vendors, integrators, or suppliers to ensure they can effectively handle incidents involving embedded components and devices. [SP800-82r3] • Follow the transit operator's response plan for incident reporting, which outlines who to notify both internally and externally, what details to include, and the expected timeframe for completing those actions. • Use technology, where feasible, to expedite incident reporting. [SP800-61r3]	IR-06 IR-07 IR-08 SR-08
RS.CO-02: Internal and external stakeholders are notified of incidents	E	E	—	**1, 2:** Effective incident communications rely on notifications to stakeholders to promote collaboration. When responding to large-scale or large-impact incidents that could compromise transit agency assets, reporting and communication are crucial. Transit operators should understand their notification requirements and/or policies and be prepared to alert internal and external parties, as required. For transit agencies/operators, OT and IT assets may be the responsibility of a single office or role, while for others, they may be split between different offices or roles, requiring a	IR-04 IR-06 IR-07 SR-03 SR-08

NIST CSF 2.0 Subcategory	1. Protection and Management of Assets	2. Stakeholder Coordination	3. Organizational Development	Subcategory Rationale, Considerations, and Guidelines	Informative References
				transit agency to establish capabilities to disseminate notifications among different owners. Internal stakeholders (e.g., the organization's workforce) should have training that prepares and enables them with appropriate methods to respond to an incident. Transit agencies may also need to report to external stakeholders (e.g., vendors, supply chain partners, local law enforcement, and passengers) during incident response to allow for external collaboration and asset protection. **Considerations and Guidelines:** • Consider maintaining documented policies and procedures specifying the appropriate external entities to whom confirmed cybersecurity incidents must be reported, such as state or federal regulators, customers, Sector Risk Management Agencies (as required), ISACs/ISAOs, and CISA, as well as the methods for reporting. [CISA-CPGs] • Provide information to appropriate staff (e.g., analysts) for evidence gathering, investigation, and recommendations on the best course of action. [APTA-SS-CCS-RP-006-23] • Report known incidents to CISA and other relevant parties within the time frames specified by applicable regulatory guidance, or, if no guidance exists, as soon as it is safely possible to do so. [CISA-CPGs], [TSA-SD-1582-21-01C] [6] • Coordinate with and notify internal and external stakeholders of incidents consistent with incident response strategy and capabilities. Internal personnel and external stakeholders (e.g., supply chain partners, vendors, external service providers) may have roles in reporting, responding, and mitigating declared incidents. Agencies may use tracking systems to notify and coordinate with appropriate personnel and stakeholders (internal and external), especially if there are established notification agreement requirements on compromises and potential compromises. Coordinate and perform notifications with appropriate	CISA CPG 5.B

[6] It is important to note that not all organizations are bound by the TSA Security Directive (SD). This requirement applies specifically to certain transit agencies.

NIST CSF 2.0 Subcategory	1. Protection and Management of Assets	2. Stakeholder Coordination	3. Organizational Development	Subcategory Rationale, Considerations, and Guidelines	Informative References
				stakeholders who may have a role in incident coordination or response. [SP800-61r3]	
RS.MI-01: Incidents are contained	—	E	—	**2:** To contain incidents and prevent further spread or impact to other systems that contain sensitive data or to IT or OT systems and assets, transit agencies should plan to coordinate the response with relevant stakeholders. These coordination plans may extend to vendors and supply chain partners, depending on the extent of the incident and the parties' roles. Transit agencies may include requirements in contracts or agreements (e.g., MOUs) to identify, codify, and enforce stakeholder expectations, roles, and responsibilities, which supports incident mitigation efforts. **Recommendations/Guidelines/Considerations:** • Develop an incident response plan to proactively detect, contain, eradicate and recover from a security breach. [APTA-SS-ECS-RP-001-14R1] • Consider how the organization would respond, and the additional time required to coordinate the response, for incidents in which OT components are physically remote and not continually staffed. The system may need to be designed with the ability to minimize impacts until personnel arrive on-site (e.g., remote shutdown or disconnects). [SP800-82r3] • Understand that cyber incident mitigation may involve process shutdowns or communication disconnects that impact operations and communicate these impacts during incident mitigation. [SP800-82r3] • Implement containment procedures to prevent additional damage. Consider if technologies or their features can be configured to support aspects of automatic containment in addition to incident handlers performing containment. [SP800-61r3]	IR-04

5.6. Recover

Table 12 Subcategory-level Guidelines for the Recover Function

NIST CSF 2.0 Subcategory	1. Protection and Management of Transit Assets	2. Stakeholder Coordination	3. Organizational Development	Subcategory Rationale, Considerations, and Guidelines	Informative References
RC.RP-01: The recovery portion of the incident response plan is executed once initiated from the incident response process	E	E	E	**1:** Recovery after a cybersecurity incident should be approached systematically, with a focus on restoring critical operational capabilities to minimize service disruptions and ensure passenger safety. The primary focus for recovery should be getting transit systems back online, with a clear emphasis on the tools and systems directly involved in service delivery, such as signaling systems, vehicle operations, and fare collection equipment. The order of recovery should be prioritized based on the impact to safety, service continuity, and passenger experience. **2, 3:** Recovery plans should be developed, regularly maintained, and tested to ensure they remain current and effective in supporting recovery efforts after an incident, and to prevent outdated information or guidance. Additionally, transit operators must consider requirements outlined in contracts, MOUs, and other supplier agreements related to recovery and restoration and ensure third-party vendors and suppliers are aware of recovery expectations and protocols to support seamless recovery/reconstitution. Transit operators can enhance organizational resilience by using different forms of workforce training (e.g., tabletop exercise, unannounced testing) to strengthen the skills and procedures necessary for effective incident recovery.	CP-10 IR-04 IR-08 CISA CPG 6.A

NIST CSF 2.0 Subcategory	1. Protection and Management of Transit Assets	2. Stakeholder Coordination	3. Organizational Development	Subcategory Rationale, Considerations, and Guidelines	Informative References
				Considerations and Guidelines: • Develop, maintain, and execute plans to recover and restore to service any business- or mission-critical assets or systems that might be impacted by a cybersecurity incident. [CISA-CPGs] • Ensure that all staff (including external suppliers and vendors) involved in recovery and reconstitution coordinate and respond based on the incident response plan or playbook. [SP800-61r3] • Restore systems within a predefined time-period (as defined in contingency plans) from configuration-controlled and integrity-protected information representing a known, operational state for the system and its components. • Track the actual time that critical services were unavailable or diminished, comparing the actual outage with agreed-upon service levels and recovery times. [SP800-184] • Validate that restored assets and systems are fully functional and meet the security requirements of the transit agency. [SP800-184] • Routinely test a transit agency's ability to recover and restore system functionality. [APTA-SS-SEM-S-004-09R2] • Leverage NIST SP 800-184 for additional guidance on incident recovery plans and plan execution. [SP800-184]	
RC.RP-03: The integrity of backups and other restoration assets is verified before using them for restoration	E	—	—	**1:** Attackers may target primary systems, assets, and data and attempt to compromise or modify backups. The reliability and usability of backups directly affect a transit operator's ability to maintain operations after an incident. Transit operators should ensure that assets are restored from clean backups, including offline backups, that are free from corruption or integrity issues. This verification must take place	CP-02 CP-04 CP-09

NIST CSF 2.0 Subcategory	1. Protection and Management of Transit Assets	2. Stakeholder Coordination	3. Organizational Development	Subcategory Rationale, Considerations, and Guidelines	Informative References
				before beginning the restoration process, particularly for assets critical to workforce and rider safety or when urgent restoration is required during an active incident. **Considerations and Guidelines:** • Maintain regular backups of system data and implement, review, and enforce policies on backups. [APTA-SS-ECS-RP-001-14R1] • Check restoration assets for indicators of compromise, file corruption, and other integrity issues before use. [SP800-61r3], [IR8374], [TSA-SD-1582-21-01C][7]	
Incident Recovery Communication (RC.CO): Restoration activities are coordinated with internal and external parties					
RC.CO-03: Recovery activities and progress in restoring operational capabilities are communicated to designated internal and external stakeholders	—	E	E	**2:** Effective communication with stakeholders is crucial during recovery efforts, as it helps maintain situational awareness, restore confidence in transit operations, ensure passenger safety, and support decision-making and resource allocation. Regular and ongoing updates about recovery activities and progress should be provided to all stakeholders involved in or affected by the recovery process. If standard communication channels are disrupted during a cyber incident, alternative methods such as phone lines, messaging apps, or social media platforms should be used to stay connected with staff and customers. Additionally, recovery efforts may include managing after-action activities, such as collaborating with external stakeholders (e.g., vendors, supply chain partners) to assess and address potential supply chain disruptions. **3:** During a cyber event, it is important that the workforce knows how, when, and with whom to communicate about the incident. This reduces confusion, prevents the spread of misinformation, and enables the right people to take appropriate action. It	IR-04 IR-06 SR-08

[7] It is important to note that not all organizations are bound by the TSA Security Directive (SD). This requirement applies specifically to certain transit agencies.

NIST CSF 2.0 Subcategory	1. Protection and Management of Transit Assets	2. Stakeholder Coordination	3. Organizational Development	Subcategory Rationale, Considerations, and Guidelines	Informative References
				also supports coordinated incident response, protects sensitive information, and helps maintain the safety and trust of staff, customers, and other stakeholders. **Considerations and Guidelines:** • Identify in the Cybersecurity Incident Response Plan who (by position) is responsible for implementing specific measures, including communications during incident recovery, and any necessary resources needed to implement these measures. [TSA-SD-1582-21-01C] [8] • Establish and adhere to a crisis communications plan, including procedures for reporting incident status to personnel and templates for public press releases. [APTA-SS-ECS-RP-001-14R1] • Communicate recovery efforts to the public in accordance with the incident response or contingency plan. • Direct any press inquiries regarding an investigation of a cyber incident to the organization’s designated public information officer. [APTA-RT-OP-S-002-02R4] • Keep employees and the public updated on system recovery status through public awareness messages via social media and other communication tools, and coordinate messaging with public information officers. [APTA-SS-ISS-RP-007-24] • Abide by rules and protocols established in contracts related to information sharing with suppliers. [SP800-61r3]	

[8] It is important to note that not all organizations are bound by the TSA Security Directive (SD). This requirement applies specifically to certain transit agencies.

References

[49-CFR-1582.113] Code of Federal Regulations, Title 49, *Transportation*, Section 1582.113, *Security training program general requirements*. (49 C.F.R. § 1582.113) https://www.ecfr.gov/current/title-49/subtitle-B/chapter-XII/subchapter-D/part-1582/subpart-B/section-1582.113

[APTA-RT-OP-S-002-02R4] American Public Transportation Association (APTA) (2025) Rail Transit Systems (RT), Operating Practices (OP). Standard (S). APTA RT-OP-S-002-02, Rev. 4, *Rail Transit Accident/Incident Notification and Investigation Requirements*. https://www.apta.com/wp-content/uploads/APTA-RT-OP-S-002-02_R4.pdf

[APTA-SS-CCS-RP-001-10] American Public Transportation Association (APTA) (2010) Security for Transit Systems (SS), Control and Communications Security (CCS). Recommended Practice (RP). APTA SS-CCS-RP-001-10, *Securing Control and Communications Systems in Transit Environments Part 1: Elements, Organization and Risk Assessment/Management*. https://www.apta.com/wp-content/uploads/Standards_Documents/APTA-SS-CCS-RP-001-10.pdf

[APTA-SS-CCS-RP-002-13] American Public Transportation Association (APTA) (2013) Security for Transit Systems (SS), Control and Communications Security (CCS). Recommended Practice (RP). APTA SS-CCS-RP-002-13, *Securing Control and Communications Systems in Rail Transit Environments Part II: Defining a Security Zone Architecture for Rail Transit and Protecting Critical Zones*. https://www.apta.com/wp-content/uploads/Standards_Documents/APTA-SS-CCS-RP-002-13.pdf

[APTA-SS-CCS-RP-004-16] American Public Transportation Association (APTA) (2016) Security for Transit Systems (SS), Control and Communications Security (CCS). Recommended Practice (RP). APTA-SS-CCS-RP-004-16*, Securing Control and Communications Systems in Rail Transit Environments Part IIIb: Protecting the Operationally Critical Security Zone*. https://www.apta.com/wp-content/uploads/Standards_Documents/APTA-SS-CCS-RP-004-16.pdf

[APTA-SS-CCS-RP-006-23] American Public Transportation Association (APTA) (2023) Security for Transit Systems (SS), Control and Communications Security (CCS). Recommended Practice (RP). APTA SS-CCS-RP-006-23*, Operational Technology Cybersecurity Maturity Framework*

(OT-CMF) Overview. https://www.apta.com/wp-content/uploads/APTA-SS-CCS-RP-006-23.pdf

[APTA-SS-CCS-WP-005-19] American Public Transportation Association (APTA) (2021) Security for Transit Systems (SS), Control and Communications Security (CCS). White Paper. APTA SS-CCS-WP-005-19, *Securing Control and Communications Systems in Transit Bus Vehicles and Supporting Infrastructure*. https://www.apta.com/wp-content/uploads/APTA-SS-CCS-WP-005-19.pdf

[APTA-SS-ECS-RP-001-14R1] American Public Transportation Association (APTA) (2022) Security for Transit Systems (SS), Enterprise Cyber Security (ECS). Recommended Practice (RP). APTA SS-ECS-RP-001-14, Rev. 1, *Cybersecurity Considerations for Public Transit*. https://www.apta.com/wp-content/uploads/APTA-SS-ECS-RP-001-14_R1.pdf

[APTA-SS-ECS-RP-003-19] American Public Transportation Association (APTA) (2019) Security for Transit Systems (SS), Enterprise Cyber Security (ECS). Recommended Practice (RP). APTA SS-ECS-RP-003-19, *Enterprise Cybersecurity Involving the Board of Directors and the Executive Suite*. https://www.apta.com/wp-content/uploads/APTA-SS-ECS-RP-003-19.pdf

[APTA-SS-ECS-RP-004-23] American Public Transportation Association (APTA) (2023) Security for Transit Systems (SS), Enterprise Cyber Security (ECS). Recommended Practice (RP). APTA SS-ECS-RP-004-23, *Developing a Cybersecurity Program That Meets an Agency's Needs*. https://www.apta.com/wp-content/uploads/APTA-SS-ECS-RP-004-23.pdf

[APTA-SS-ISS-RP-003-23] American Public Transportation Association (APTA) (2023) Security for Transit Systems (SS), Infrastructure & Systems Security (ISS). Recommended Practice (RP). APTA SS-ISS-RP-003-23, *Sensitive Security Information Policy*. https://www.apta.com/wp-content/uploads/APTA-SS-ISS-RP-003-23.pdf

[APTA-SS-ISS-RP-007-24] American Public Transportation Association (APTA) (2024) Security for Transit Systems (SS), Infrastructure & Systems Security (ISS). Recommended Practice (RP). APTA SS-ISS-RP-007-24, *Security Measures for Elevated Threats*. https://www.apta.com/wp-content/uploads/APTA-SS-ISS-RP-007-24.pdf

[APTA-SS-ISS-RP-008-24] American Public Transportation Association (APTA) (2024) Security for Transit Systems (SS), Infrastructure & Systems Security (ISS). Recommended Practice (RP). APTA SS-ISS-RP-008-

24, *Safety and Security Certification*. https://www.apta.com/wp-content/uploads/APTA-SS-ISS-RP-008-24.pdf

[APTA-SS-SEM-S-004-09R2] American Public Transportation Association (APTA) (2022) Security for Transit Systems (SS), Security and Emergency Management (SEM). Standard (S). APTA SS-SEM-S-004-09, Rev. 2, *Transit Exercises*. https://www.apta.com/wp-content/uploads/APTA-SS-SEM-S-004-09_R2.pdf

[APTA-SS-SIS-S-010-13R1] American Public Transportation Association (APTA) (2023) Security for Transit Systems (SS), Infrastructure Security (SIS). Standard (S). APTA SS-SIS-S-010-13, Rev. 1, *Security Considerations for Public Transit*. https://www.apta.com/wp-content/uploads/APTA-SS-SIS-S-010-13_R1.pdf

[APTA-SS-SIS-S-017-21] American Public Transportation Association (APTA) (2021) Security for Transit Systems (SS), Infrastructure Security (SIS). Standard (S). APTA SS-SIS-S-017-21, *Security Risk Assessment Methodology for Public Transit*. https://www.apta.com/wp-content/uploads/APTA-SS-SIS-S-017-21.pdf

[APTA-SS-SRM-RP-005-12R1] American Public Transportation Association (APTA) (2021) Security for Transit Systems (SS), Security Risk Management (SRM). Recommended Practice (RP). APTA SS-SRM-RP-005-12, Rev. 1, *Security Awareness Training*. https://www.apta.com/wp-content/uploads/APTA-SS-SRM-RP-005-12_R1.pdf

[APTA-SUDS-TAM-RP-010-21] American Public Transportation Association (APTA) (2021) Sustainability and Urban Design (SUDS), Transit Asset Management (TAM). Recommended Practice (RP). APTA-SUDS-TAM-RP-010-21, *Using Asset Criticality to Make More Informed Decisions in a Transit Agency*. https://www.apta.com/wp-content/uploads/APTA-SUDS-TAM-RP-010-21.pdf

[CISA-CPGs] U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) Cross-Sector Cybersecurity Performance Goals 2.0 (CPGs 2.0). https://www.cisa.gov/cybersecurity-performance-goals-2-0-cpg-2-0

[CSF2.0] National Institute of Standards and Technology (2024) *The NIST Cybersecurity Framework (CSF) 2.0.* (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) 29. https://doi.org/10.6028/NIST.CSWP.29

[IR8179] National Institute of Standards and Technology (2018) NIST Internal Report (IR) 8179, *Criticality Analysis Process Model: Prioritizing Systems and Components*. (National Institute of

Standards and Technology, Gaithersburg, MD), NIST Internal Report (NIST IR) 8179. https://doi.org/10.6028/NIST.IR.8179

[IR8183r2] Stouffer K, Pease M, Tang CY, Zimmerman T, Thompson M, Sherule A, Silva ZL, Quigg K (2025) *Cybersecurity Framework Version 2.0 Manufacturing Profile*. (National Institute of Standards and Technology, Gaithersburg, MD), NIST IR (Internal Report) NIST IR 8183r2 ipd. https://doi.org/10.6028/NIST.IR.8183r2.ipd

[IR8276] National Institute of Standards and Technology (2018) NIST Interagency or Internal Report (IR) 8276, *Key Practices in Cyber Supply Chain Risk Management: Observations from Industry*. https://doi.org/10.6028/NIST.IR.8276

[IR8374] National Institute of Standards and Technology (2025) *Ransomware Risk Management: A CSF 2.0 Community Profile.* (National Institute of Standards and Technology, Gaithersburg, MD), NIST Internal Report (NIST IR) 8374r1, ipd. https://nvlpubs.nist.gov/nistpubs/ir/2025/NIST.IR.8374r1.ipd.pdf

[SP1305] National Institute of Standards and Technology (2024) *NIST Cybersecurity Framework 2.0: Quick-Start Guide for Cybersecurity Supply Chain Risk Management (C-SCRM).* (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 1305. https://doi.org/10.6028/NIST.SP.1305

[SP1800-23] National Institute of Standards and Technology (2020) *Energy Sector Asset Management For Electric Utilities, Oil & Gas Industry. (National Institute of Standards and Technology*. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 1800-23. Complete Guide. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-23.pdf

[SP800-53r5] Joint Task Force Transformation Initiative (2020) *Security and Privacy Controls for Information Systems and Organizations*. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 5. https://doi.org/10.6028/NIST.SP.800-53r5

[SP800-61r3] Nelson A, Rekhi S, Souppaya M, Scarfone K (2025) *Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile*. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-61r3. https://doi.org/10.6028/NIST.SP.800-61r3

[SP800-82r3] Stouffer K, Pease M, Tang CY, Zimmerman T, Pillitteri V, Lightman S, Hahn A, Saravia S, Sherule A, Thompson M (2023) *Guide to Operational Technology (OT) Security*. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-82r3. https://doi.org/10.6028/NIST.SP.800-82r3

[SP800-100] Bowen P, Hash J, Wilson M (2006) *Information Security Handbook: A Guide for Managers*. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-100, Includes updates as of March 7, 2007. https://doi.org/10.6028/NIST.SP.800-100

[SP800-184] National Institute of Standards and Technology (2016) *Guide for Cybersecurity Event Recovery*. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-184. https://doi.org/10.6028/NIST.SP.800-184

[TSA-SD-1582-21-01C] U.S. Department of Homeland Security (DHS) Transportation Security Administration (TSA) (2024) Security Directive (SD) 1582-21-01C, *Enhancing Public Transportation and Passenger Railroad Cybersecurity*. https://www.tsa.gov/sites/default/files/security_directive_1582-21-01c_and_memo_508c.pdf

Appendix A. Selected Bibliography

[1] Pascoe C, Snyder JN, Scarfone KA (2024) NIST Cybersecurity Framework 2.0: A Guide to Creating Community Profiles. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) NIST CSWP 32 ipd. https://doi.org/10.6028/NIST.CSWP.32.ipd

[2] Tang C, Division E, Alshtein A, Hardison M, Sames C (2025) Developing a Transit Cybersecurity Framework Community Profile Project Update. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) NIST CSWP 35 ipd. https://doi.org/10.6028/NIST.CSWP.51.ipd

[3] National Institute of Standards and Technology (2021) Managing the Security of Information Exchanges (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-47, Rev. 1. https://doi.org/10.6028/NIST.SP.800-47r1

[4] U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) Transportation Systems Sector. https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/transportation-systems-sector

[5] U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) Cross-Sector Cybersecurity Performance Goals (CPGs). https://www.cisa.gov/sites/default/files/2023-03/CISA_CPG_REPORT_v1.0.1_FINAL.pdf

[6] U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) (2025). Foundations for OT Cybersecurity: Asset Inventory Guidance for Owners and Operators. https://www.cisa.gov/sites/default/files/2025-08/joint-guide-foundations-for-OT-cybersecurity-asset-inventory-guidance_508c.pdf

[7] U.S. Department of Homeland Security (DHS) Transportation Security Administration (TSA) (2024) Notice of Proposed Rulemaking (NPRM), Enhancing Surface Cyber Risk Management. https://www.federalregister.gov/documents/2024/11/07/2024-24704/enhancing-surface-cyber-risk-management?mod=djemCybersecruityPro&tpl=cs

[8] U.S. Department of Transportation (DOT) Strategic Plan FY 2022-2026. U.S. Department of Transportation Strategic Plan FY 2022-2026

[9] American Public Transportation Association (APTA) (2019) Sustainability and Urban Design (SUDS), Transit Asset Management (TAM). Recommended Practice (RP). APTA-SUDS-TAM-RP-005-19, Improving Asset Management Through Better Asset Information. https://www.apta.com/wp-content/uploads/Standards_Documents/APTA-SUDS-TAM-RP-005-19.pdf

[10] American Public Transportation Association (APTA) (2019) Sustainability and Urban Design (SUDS), Transit Asset Management (TAM). Recommended Practice (RP). APTA-SUDS-TAM-RP-006-19, Communication and Coordination with External Stakeholders for Transit Asset Management. https://www.apta.com/wp-content/uploads/APTA-SUDS-TAM-RP-006-19.pdf

[11] American Public Transportation Association (APTA) (2023) Transit Workforce Shortage Synthesis Report. APTA-Workforce-Shortage-Synthesis-Report-03.2023.pdf

766 Appendix B. Complete CSF Subcategory Designations

NIST CSF 2.0 Subcategory	Protection and Management of Assets	Stakeholder Coordination	Organizational Development
GOVERN			
GV.OC-01: The organizational mission is understood and informs cybersecurity risk management	E	—	E
GV.OC-02: Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered	E	E	—
GV.OC-03: Legal, regulatory, and contractual requirements regarding cybersecurity — including privacy and civil liberties obligations — are understood and managed	—	—	—
GV.OC-04: Critical objectives, capabilities, and services that external stakeholders depend on or expect from the organization are understood and communicated	—	—	—
GV.OC-05: Outcomes, capabilities, and services that the organization depends on are understood and communicated	—	—	—
GV.RM-01: Risk management objectives are established and agreed to by organizational stakeholders	—	—	—
GV.RM-02: Risk appetite and risk tolerance statements are established, communicated, and maintained	E	—	—
GV.RM-03: Cybersecurity risk management activities and outcomes are included in enterprise risk management processes	—	—	—
GV.RM-04: Strategic direction that describes appropriate risk response options is established and communicated	—	—	—
GV.RM-05: Lines of communication across the organization are established for cybersecurity risks, including risks from suppliers and other third parties	—	E	E
GV.RM-06: A standardized method for calculating, documenting, categorizing, and prioritizing cybersecurity risks is established and communicated	—	—	—
GV.RM-07: Strategic opportunities (i.e., positive risks) are characterized and are included in organizational cybersecurity risk discussions	—	—	—
GV.RR-01: Organizational leadership is responsible and accountable for cybersecurity risk and fosters a culture that is risk-aware, ethical, and continually improving	—	—	E
GV.RR-02: Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced	—	E	E
GV.RR-03: Adequate resources are allocated commensurate with the cybersecurity risk strategy, roles, responsibilities, and policies	—	—	—
GV.RR-04: Cybersecurity is included in human resources practices	—	—	—
GV.PO-01: Policy for managing cybersecurity risks is established based on organizational context, cybersecurity strategy, and priorities and is communicated and enforced	E	—	E

NIST CSF 2.0 Subcategory	Protection and Management of Assets	Stakeholder Coordination	Organizational Development
GV.PO-02: Policy for managing cybersecurity risks is reviewed, updated, communicated, and enforced to reflect changes in requirements, threats, technology, and organizational mission	—	—	—
GV.OV-01: Cybersecurity risk management strategy outcomes are reviewed to inform and adjust strategy and direction	—	—	—
GV.OV-02: The cybersecurity risk management strategy is reviewed and adjusted to ensure coverage of organizational requirements and risks	—	—	—
GV.OV-03: Organizational cybersecurity risk management performance is evaluated and reviewed for adjustments needed	—	—	—
GV.SC-01: A cybersecurity supply chain risk management program, strategy, objectives, policies, and processes are established and agreed to by organizational stakeholders	—	E	—
GV.SC-02: Cybersecurity roles and responsibilities for suppliers, customers, and partners are established, communicated, and coordinated internally and externally	—	E	E
GV.SC-03: Cybersecurity supply chain risk management is integrated into cybersecurity and enterprise risk management, risk assessment, and improvement processes	—	—	—
GV.SC-04: Suppliers are known and prioritized by criticality	E	E	—
GV.SC-05: Requirements to address cybersecurity risks in supply chains are established, prioritized, and integrated into contracts and other types of agreements with suppliers and other relevant third parties	E	E	—
GV.SC-06: Planning and due diligence are performed to reduce risks before entering into formal supplier or other third-party relationships	—	—	—
GV.SC-07: The risks posed by a supplier, their products and services, and other third parties are understood, recorded, prioritized, assessed, responded to, and monitored over the course of the relationship	—	—	—
GV.SC-08: Relevant suppliers and other third parties are included in incident planning, response, and recovery activities	E	E	—
GV.SC-09: Supply chain security practices are integrated into cybersecurity and enterprise risk management programs, and their performance is monitored throughout the technology product and service life cycle	—	—	—
GV.SC-10: Cybersecurity supply chain risk management plans include provisions for activities that occur after the conclusion of a partnership or service agreement	—	—	—
IDENTIFY			
ID.AM-01: Inventories of hardware managed by the organization are maintained	E	—	—

NIST CSF 2.0 Subcategory	Protection and Management of Assets	Stakeholder Coordination	Organizational Development
ID.AM-02: Inventories of software, services, and systems managed by the organization are maintained	E	—	—
ID.AM-03: Representations of the organization’s authorized network communication and internal and external network data flows are maintained	—	—	—
ID.AM-04: Inventories of services provided by suppliers are maintained	E	E	—
ID.AM-05: Assets are prioritized based on classification, criticality, resources, and impact on the mission	E	—	—
ID.AM-07: Inventories of data and corresponding metadata for designated data types are maintained	E	—	—
ID.AM-08: Systems, hardware, software, services, and data are managed throughout their life cycles	E	—	—
ID.RA-01: Vulnerabilities in assets are identified, validated, and recorded	E	—	E
ID.RA-02: Cyber threat intelligence is received from information sharing forums and sources	—	—	—
ID.RA-03: Internal and external threats to the organization are identified and recorded	—	—	—
ID.RA-04: Potential impacts and likelihoods of threats exploiting vulnerabilities are identified and recorded	—	—	—
ID.RA-05: Threats, vulnerabilities, likelihoods, and impacts are used to understand inherent risk and inform risk response prioritization	E	—	—
ID.RA-06: Risk responses are chosen, prioritized, planned, tracked, and communicated	—	—	—
ID.RA-07: Changes and exceptions are managed, assessed for risk impact, recorded, and tracked	E	—	—
ID.RA-08: Processes for receiving, analyzing, and responding to vulnerability disclosures are established	E	E	—
ID.RA-09: The authenticity and integrity of hardware and software are assessed prior to acquisition and use	—	—	—
ID.RA-10: Critical suppliers are assessed prior to acquisition	E	E	—
ID.IM-01: Improvements are identified from evaluations	—	—	—
ID.IM-02: Improvements are identified from security tests and exercises, including those done in coordination with suppliers and relevant third parties	E	E	—
ID.IM-03: Improvements are identified from execution of operational processes, procedures, and activities	—	—	—
ID.IM-04: Incident response plans and other cybersecurity plans that affect operations are established, communicated, maintained, and improved	E	E	—
PROTECT			
PR.AA-01: Identities and credentials for authorized users, services, and hardware are managed by the organization	E	—	—
PR.AA-02: Identities are proofed and bound to credentials based on the context of interactions	—	—	—
PR.AA-03: Users, services, and hardware are authenticated	E	—	—

NIST CSF 2.0 Subcategory	Protection and Management of Assets	Stakeholder Coordination	Organizational Development
PR.AA-04: Identity assertions are protected, conveyed, and verified	—	—	—
PR.AA-05: Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties	E	—	—
PR.AA-06: Physical access to assets is managed, monitored, and enforced commensurate with risk	E	—	—
PR.AT-01: Personnel are provided with awareness and training so that they possess the knowledge and skills to perform general tasks with security risks in mind	—	—	E
PR.AT-02: Individuals in specialized roles are provided with awareness and training so that they possess the knowledge and skills to perform relevant tasks with security risks in mind	E	E	E
PR.DS-01: The confidentiality, integrity, and availability of data-at-rest are protected	E	E	—
PR.DS-02: The confidentiality, integrity, and availability of data-in-transit are protected	E	—	—
PR.DS-10: The confidentiality, integrity, and availability of data-in-use are protected	—	—	—
PR.DS-11: Backups of data are created, protected, maintained, and tested	E	—	—
PR.PS-01: Configuration management practices are established and applied	E	—	—
PR.PS-02: Software is maintained, replaced, and removed commensurate with risk	E	—	—
PR.PS-03: Hardware is maintained, replaced, and removed commensurate with risk	E	—	—
PR.PS-04: Log records are generated and made available for continuous monitoring	E	—	—
PR.PS-05: Installation and execution of unauthorized software are prevented	—	—	—
PR.PS-06: Secure software development practices are integrated and their performance is monitored throughout the software development life cycle	—	—	—
PR.IR-01: Networks and environments are protected from unauthorized logical access and usage	E	—	—
PR.IR-02: The organization’s technology assets are protected from environmental threats	E	—	—
PR.IR-03: Mechanisms are implemented to achieve resilience requirements in normal and adverse situations	E	—	—
PR.IR-04: Adequate resource capacity to ensure availability is maintained	—	—	—
DETECT			
DE.CM-01: Networks and network services are monitored to find potentially adverse events	E	—	—
DE.CM-02: The physical environment is monitored to find potentially adverse events	E	—	—

NIST CSF 2.0 Subcategory	Protection and Management of Assets	Stakeholder Coordination	Organizational Development
DE.CM-03: Personnel activity and technology usage are monitored to find potentially adverse events	—	—	—
DE.CM-06: External service provider activities and services are monitored to find potentially adverse events	E	E	—
DE.CM-09: Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events	E	—	—
DE.AE-02: Potentially adverse events are analyzed to better understand associated activities	E	—	—
DE.AE-03: Information is correlated from multiple sources	—	—	—
DE.AE-04: The estimated impact and scope of adverse events are understood	—	—	—
DE.AE-06: Information on adverse events is provided to authorized staff and tools	E	E	—
DE.AE-07: Cyber threat intelligence and other contextual information are integrated into the analysis	—	—	—
DE.AE-08: Incidents are declared when adverse events meet the defined incident criteria	—	—	—
RESPOND			
RS.MA-01: The incident response plan is executed in coordination with relevant third parties once an incident is declared	E	E	E
RS.MA-02: Incident reports are triaged and validated	—	—	—
RS.MA-03: Incidents are categorized and prioritized	—	—	—
RS.MA-04: Incidents are escalated or elevated as needed	—	—	—
RS.MA-05: The criteria for initiating incident recovery are applied	—	—	—
RS.AN-03: Analysis is performed to establish what has taken place during an incident and the root cause of the incident	—	—	—
RS.AN-06: Actions performed during an investigation are recorded, and the records' integrity and provenance are preserved	—	—	—
RS.AN-07: Incident data and metadata are collected, and their integrity and provenance are preserved	—	—	—
RS.AN-08: An incident's magnitude is estimated and validated	—	—	—
RS.CO-02: Internal and external stakeholders are notified of incidents	E	E	—
RS.CO-03: Information is shared with designated internal and external stakeholders	—	—	—
RS.MI-01: Incidents are contained	—	E	—
RS.MI-02: Incidents are eradicated	—	—	—
RECOVER			
RC.RP-01: The recovery portion of the incident response plan is executed once initiated from the incident response process	E	E	E
RC.RP-02: Recovery actions are selected, scoped, prioritized, and performed	—	—	—

NIST CSF 2.0 Subcategory	Protection and Management of Assets	Stakeholder Coordination	Organizational Development
RC.RP-03: The integrity of backups and other restoration assets is verified before using them for restoration	**E**	—	—
RC.RP-04: Critical mission functions and cybersecurity risk management are considered to establish post-incident operational norms	—	—	—
RC.RP-05: The integrity of restored assets is verified, systems and services are restored, and normal operating status is confirmed	—	—	—
RC.RP-06: The end of incident recovery is declared based on criteria, and incident-related documentation is completed	—	—	—
RC.CO-03: Recovery activities and progress in restoring operational capabilities are communicated to designated internal and external stakeholders	—	**E**	**E**
RC.CO-04: Public updates on incident recovery are shared using approved methods and messaging	—	—	—

Appendix C. List of Symbols, Abbreviations, and Acronyms

APTA
American Public Transportation Association

C-SCRM
Cyber Supply Chain Risk Management

CISA
Cybersecurity and Infrastructure Security Agency

CPG
Cybersecurity Performance Goal (CISA)

CSF
Cybersecurity Framework (NIST)

DNS
Domain Name System or Server

ISAC
Information Sharing and Analysis Center

ISAO
Information Sharing and Analysis Organization

ISS
Infrastructure & Systems Security (APTA Standards Topic)

IT
Information Technology

MFA
Multifactor Authentication

MOU
Memorandum of Understanding

MSSP
Managed Security Service Provider

NCCoE
National Cybersecurity Center of Excellence

NIST
National Institute of Standards and Technology

OT
Operational Technology

PCI DSS
Payment Card Industry Data Security Standard

PHI
Protected Health Information

PII
Personally Identifiable Information

PLC
Programmable Logic Controller

RP
Recommended Practice (APTA)

SCADA
Supervisory Control and Data Acquisition

SD
Security Directive (TSA)

SDLC
System Development Life Cycle

SIPOC
Suppliers, Inputs, Processes, Outputs, Customers

SLA
Service Level Agreement

SME
Subject Matter Expert

SMTA
Small- and Medium-sized Transit Agencies

SOC
Security Operations Center

SP
Special Publication (NIST)

SRM
Security Risk Management (APTA Standards Topics)

SSI
Sensitive Security Information

SSL
Secure Socket Layer

TLS
Transport Layer Security

TSA
Transportation Security Administration

TTPs
Tactics, Techniques, and Procedures

TVA
Threat and Vulnerability Assessment

USB
Universal Serial Bus