APTA STANDARDS PROGRAM

RECOMMENDED PRACTICE

APTA SS-CCS-RP-006-23

First Published: May 23, 2023

Control and Communications Security Working Group

Operational Technology Cybersecurity Maturity Framework (OT-CMF) Overview

Part 1: Guidance in Maturing an OT Cybersecurity Program

Abstract: This document covers recommended practices for developing and growing an operational technology (OT) cybersecurity maturity program.

Keywords: building automation systems (BAS), bus depot, cybersecurity, industrial control systems (ICS), operational technology (OT), Operational Technology Cybersecurity Maturity Framework (OT-CMF), radio, signaling, supervisory control and data acquisition (SCADA) systems, communications-based train control (CBTC), transit vehicle.

Summary: This document presents an overview and guidance to assist transit agencies in maturing their OT cybersecurity programs. The guidance walks through the six levels of maturity starting with Level 0, which is an on-ramp to launch an OT cybersecurity program.

Foreword

The American Public Transportation Association is a standards development organization in North America. The process of developing standards is managed by the APTA Standards Program's Standards Development Oversight Council (SDOC). These activities are carried out through several standards policy and planning committees that have been established to address specific transportation modes, safety and security requirements, interoperability, and other topics.

APTA used a consensus-based process to develop this document and its continued maintenance, which is detailed in the manual for the APTA Standards Program. This document was drafted in accordance with the approval criteria and editorial policy as described. Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

This document was prepared by the Control and Communications Security Working Group as directed by the Security Standards Policy and Planning Committee.

This document represents a common viewpoint of those parties concerned with its provisions, namely transit operating/planning agencies, manufacturers, consultants, engineers and general interest groups. The application of any recommended practices or guidelines contained herein is voluntary. APTA standards are mandatory to the extent incorporated by an applicable statute or regulation. In some cases, federal and/or state regulations govern portions of a transit system's operations. In cases where there is a conflict or contradiction between an applicable law or regulation and this document, consult with a legal adviser to determine which document takes precedence.

This is a new document.

Table of Contents

List of Figures and Tables

Participants

The American Public Transportation Association greatly appreciates the contributions of sub-committee chair **Muneer Baig**; sub-committee members **Ahmed Idrees**, **John Moore**, **Tim Coogan**, **Rafi Khan**, **Dr. Julius Smith**, **Dennis Story**, **Roman Vitkovitsky** and **Dr. Jerry Joyce**; and CCSWG committee facilitator **Michael Echols**, who provided the primary effort in the drafting of this document.

At the time this standard was completed, the Control and Communications Security Working Group included the following members:

Ahmed Idrees, Sound Transit, *Chair*
Muneer Baig, SysUSA, *Vice Chair*
John Moore, Phoenix Contact, *Secretary*

Rotem Abeles, *Cylus*
Lee Allen, *TSA*
Dawn Armstrong, *Virginia Hyperloop*
Rebecca Ash, *TSA*
Alesia Cain, *Macro*
Melvina Beard, *Denver RTD*
Robert Brown, *Razor Secure*
Tom Burns, *Kawasaki Rail*
Tim Coogan, *Denver RTD*
Rachel Deen, *Transit Safety Solutions*
Ali Edraki, *Wabtec*
Ted Ellis, *Sound Transit*
Chris Heil, LTK *Consulting*
Susan Howard, *Jacobs*
Jerry Joyce, *Hatch LTK*
Asaf Kalderon, *CyberX Lab*
Bilal Khan, *NJ Transit*
Rafi Khan, *NJ Transit*
Tri Le, Armand *Consulting*
Kyle Malo, *WMATA*
Bruce Middleton, *Alstom*
Sheri Ricardo, *Alliance for Sustainable Energy*
Alan Rowe, *Forcing Function*
Mark Salsberg, *WGD Consulting*
Martin Schroeder, *Jacobs*
Leonard (Chris) Shepherd, *Gannett Fleming*
Scott Sherin, Alstom *Group*
Jack Sherman, *Hampton Roads Transit*
Miki Shifman, *Cylus*
Mark Shtern, *WGD Consulting*
Julius Smith, *DART*
Dennis Story, *HART*
Alfredo Perez, *Perez Consulting*
Roman Vitkovitsky, *WMATA*

Project team
Polly Hanson, *American Public Transportation Association*
Michael A. Echols, *Max Cybersecurity LLC, CCSWG facilitator*

Introduction

This introduction is not part of APTA SS-CCS-RP-006-23, "Operational Technology Cybersecurity Maturity Framework (OT-CMF) Overview."

APTA recommends the use of this document by:

- individuals or organizations that operate rail transit systems;
- individuals or organizations that contract with others for the operation of rail transit systems; and
- individuals or organizations that influence how rail transit systems are operated (including but not limited to consultants, designers and contractors).

Scope and purpose

This recommended practice is not intended to supplant existing safety or security standards or regulations but to supplement and provide additional guidance to mature OT cybersecurity programs. Passenger transit agencies and the vendor community now evolve their security requirements and system security features independently. The purpose of this recommended guidance is to organize best practices into a systematic approach for transit agencies to launch, grow and sustain an OT cybersecurity program. This recommended practice sets minimum requirements for control security within the transit industry; helps to standardize control and operations system practices; and promotes the adoption of voluntary industry best practices in control security.

Operational Technology Cybersecurity Maturity Framework (OT-CMF) Overview

Part 1: Guidance in Developing and Maturing OT Cybersecurity Programs

1. About this series

This recommended practice is the first of a series of documents that will be updated on a regular cycle to keep them current. This document provides guidance on how to apply the security best practices found in the OT-CMF to an OT environment. The guidance is broken into six tier levels that represent OT program maturity. For each step within a tier level, there is a brief discussion of how to interpret and apply the guidance in such environments, along with any unique considerations or differences from common IT environments. The applicability is addressed, and additional steps needed to manage OT environments are explained.

OT usually has a physical and a real-time component, such as controlling the operation of an automated assembly line or chemical reactor. Sometimes the acronym "ICS" (industrial control systems) is used as a synonym for this subject, but OT has become more popular in today's industrial environments; many critical digital components such as network switches don't qualify as control systems in the strict sense. This recommended practice uses only "OT" with the understanding that ICS is covered as well.

This document is a companion document to the OT-CMF chart and security controls description in the appendix. The goal of this framework is to make it easy for an agency to voluntarily assess their OT security program and mature it over time. The OT-CMF overview identifies the steps that an agency follows to set up a successful program. This recommended practice presents a methodology for securing transit communications and control systems; defines an on-ramp for a program; and presents an approach to systematically mature an OT cybersecurity program.

A more instructional APTA guide and a deeper set of OT-CMF building blocks is available in the supporting document to this one, "Securing Control and Communications Systems in Transit Environments: Implementing the OT-CMF." The new supporting document was previously numbered as APTA-CCS-RP-001-10, "Part 1: Elements, Organization and Risk Assessment/Management." It will be referred to in this document as the APTA–OT-CMF Implementation Guide.

Throughout the supporting document, the APTA–OT-CMF Implementation Guide, the elements of building and maturing an OT cybersecurity program are defined to support use of this document, "Operational Technology Cybersecurity Maturity Framework (OT-CMF) Overview."

Within this document, for each step within a tier level, there is a brief discussion of how to interpret and apply the best practice in such environments, along with any unique considerations or differences from common IT environments. The applicability is addressed, and additional steps needed to manage OT environments are explained accordingly.

1.1 Intent of the series

The intent of this document is to provide a framework that enables and empowers transit agencies to plan, implement, measure, monitor and mature an OT cybersecurity program that is responsive to evolving threats. This recommended practice spearheads an effort within APTA to extend cybersecurity best practices to the transit industry. It represents the contribution of leading-edge information from transit agencies that already have a control security program, as well as recommendations from agencies that are trying to launch programs. Information in the document is mainly derived from the U.S. Department of Homeland Security (DHS), the Cybersecurity and Infrastructure Security Agency (CISA), the Transportation Security Administration (TSA), the National Institute of Standards and Technology (NIST), vendors who serve the transportation and IT communities, and professionals and experts from the cybersecurity field.

This recommended practice is not intended to supplant existing safety or security standards and regulations. Instead, it provides an overview of the critical need to follow those best practices and to invest in standardization of OT cybersecurity programs. This guide should help to fill potential gaps in current OT programs and promote standards implementation at transit agencies.

1.2 Background

The OT-CMF is based on NIST best practices and incorporates elements of leading standards important to OT environments. This recommended practice is the guidance for using the OT-CMF. The target OT-CMF maturity of any transit organization will be commensurate with revenue, passengers per year, mission, corporate risk tolerance and culture. Although maturity Level 3 should be the target of all transit agencies, a goal of the OT-CMF is to assist all transit agencies to at least start an OT security program.

Today's reality is that while a high dependence on legacy OT still exists, many critical infrastructure system asset owners are migrating to interconnected technologies. As a result, transit systems manage large numbers of control and communications systems that must interoperate to provide seamless service to the public. Transit organizations interconnect systems to incorporate new technologies, delivering innovations that increase operational efficiencies, increase safety, and enable data sharing and reporting with other groups within and outside the organization to enhance performance and reliability.

APTA initiated the development of an OT-CMF through its CCSWG, following a TSA and DHS recommendation to standardize transportation OT cybersecurity practices. This maturity framework is based on NIST best practices and incorporates elements of standards important to OT cybersecurity. OT systems manage, command, direct or regulate the behavior of devices used in industrial systems supporting operational and safety-critical functions. Managing the security of OT systems can be a challenge and is currently performed in many ways across the industry.

Standardization in approach to maturing an OT cybersecurity program will create opportunities for transit agencies to work together and share lessons learned. The challenges in building a program around these interconnected systems—which were never designed or envisioned to be connected—are great. Additionally, some new OT systems coming online at transit agencies are designed to be networked, but they do not readily accept all the security techniques employed for enterprise technology or business systems. The main issue is that OT is based on system functionality, reliability and availability. When typical security techniques are applied, they often interfere with these basic tenets of OT systems. A holistic approach to management and growth of the environment must account for OT nuances and risk, present and future. However, often an understanding of OT requirements is lacking across most agencies.

Attempting to mitigate risks to OT networks and systems simply by deploying IT security technologies into a control system environment is not a viable solution. Although newer OT products often use the same

underlying protocols used in IT and business networks, the nature of the control systems' reliance on functionality—combined with operational and availability requirements—may make even ubiquitous security technologies, such as antivirus, inappropriate. Some sectors, such as energy, transportation and chemical, have time-sensitivity requirements. Latency and throughput issues introduced by security solutions may cause unacceptable delays and degrade or prevent optimal system performance. A security prevention technique used for IT may disrupt the functions and performance of the OT.

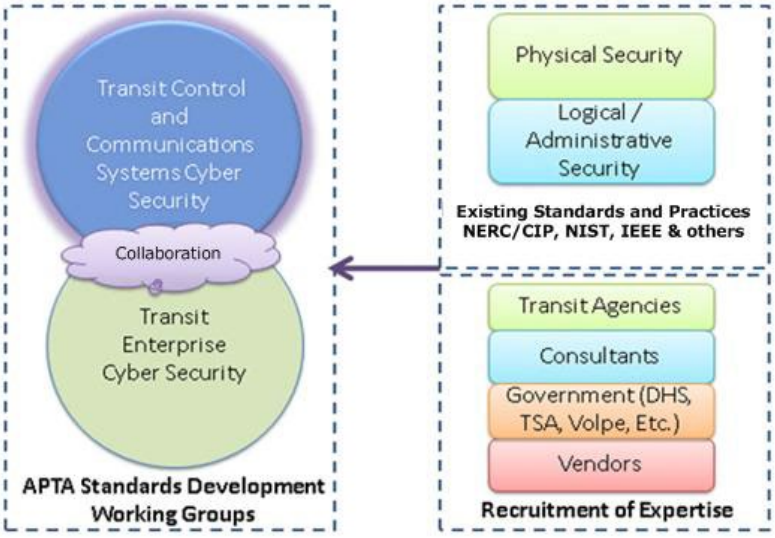
The OT-CMF is not a shortcut, simple solution or "silver bullet" to solve cybersecurity vulnerability issues across OT environments. Efficiently addressing OT cybersecurity issues requires a clear understanding of the current security state, emerging security challenges, and specific defensive countermeasures for the operator or user. A holistic approach—one that uses specific activities based on best practices that is implemented in layers can assist to create the desired and aggregated, risk-based OT security posture. All transit agencies with OT should have a cybersecurity maturity process. The activities to secure the environment also create an opportunity for increasing performance and begin a process to better evaluate security controls.

1.2.1 APTA's approach

APTA has divided working groups examining the cybersecurity awareness and vulnerability mitigation effort into two teams (see **Figure 1**):

- Control and Communications Security Working Group (CCSWG)
- Enterprise Cybersecurity Working Group (ECSWG)

FIGURE 1
The APTA Total Effort in Transportation Cybersecurity



1.2.1.1 Control and Communications Security Working Group

The CCSWG draws upon existing standards from the North American Electric Reliability Corporation's Critical Infrastructure Protection program (NERC-CIP), NIST, Internet Security Alliance, the Institute of Electrical and Electronics Engineers (IEEE), physical security knowledge, and logical/administrative security. Additional subject matter experts (SMEs) from transit agencies; transit vendors; government departments including DHS, TSA and the John A. Volpe National Transportation Systems Center; and consultants participate in defining and reviewing recommended practices and guidelines. The CCSWG stays abreast of

developments related to the Center for Internet Security (CIS) Controls, the MITRE ATT&CK Framework and NIST Cybersecurity Framework (NIST CSF).

1.2.1.2 Enterprise Cybersecurity Working Group

The ECSWG develops APTA standards pertaining to mass transit cybersecurity. Specifically, it provides strategic recommendations for chief information officers and decision-makers regarding business cybersecurity, information systems, fare collection and general cybersecurity technologies. The ECSWG also uses cybersecurity best practices and industry standards to draw upon for securing the enterprise system and components, including but not limited to NIST, CIS system controls and hardening guidance, OWASP security code practices, and payment card industry data security standards.

In practice, the recommendations from the ECSWG and CCSWG must mesh to ensure that the integration of the control systems and enterprise systems connect securely. There are many frameworks for maturing enterprise systems. This is one of the first frameworks for transit OT maturity.

2. The need for an OT cybersecurity maturity framework

2.1 Overview

A transit agency is a very complex organization that has assets and equipment controlled by supervisory systems with communications mechanisms in office buildings, depots, hubs, stations and along railroad tracks. These systems, used both to control and communicate, are located along the routes in wayside bungalows, stations, roadways, signal houses, tunnels, maintenance yards, power stations, refueling depots, equipment storage yards/parking lots, storage depots, local control rooms, and operations control rooms.

For each step within the six tiers of the framework, there is a brief discussion of how to interpret and apply the guidance in such environments, along with any unique considerations or differences from common IT environments. The applicability of actions to mature the OT program is addressed, and additional steps needed in OT environments to safely apply concepts are also explained.

There are real risks associated with not having an OT cybersecurity program, including safety concerns with not having a grasp of interdependencies as well as visibility to manage and build resilience in the OT environment. The performance and survivability of OT systems is determined by real-time requirements and sensitive software that requires unique methods of upgrade, patching and controls management. This in turn drives the priority of the security requirements (e.g., availability, integrity and confidentiality of process data).

2.2 Understanding cybersecurity maturity

It is important to understand the context of developing cybersecurity maturity. The OT-CMF is a tool for transit agencies and not a judgment statement. To secure the sector, transit agencies must be able to discuss the policy and technology approach that right-sizes the best practices produced by NIST, CISA and other leading standards organizations. Most transit agencies will never reach Level 4 or Level 5. The goal should be for transit agencies to reach Level 3 maturity.

Level 3 maturity will ensure that agencies have leadership, policies, procedures, management, evaluation programs and response capabilities. Level 4 is designed to guide agencies to optimize and integrate artificial intelligence with automation of controls. The Level 5 expectations are a goal of the future, where optimization also includes presenting decision-makers with curated information for making policy and risk adjustments that the system autonomously implements. There will be agencies with capabilities in the next higher maturity level. The agency cannot claim they are at a level unless they are performing all the practices successfully with that higher level. (Therefore, an agency that performs all practices of Level 3 and three practices of Level 4 is at Level 3 maturity.)

The OT-CMF is a companion to leading assessment tools. The focus of the OT-CMF is on OT and the environments harboring sensors, actuators and connectors. It is a sensitive environment that requires special attention. Some of these components are not monitored via a traditional cybersecurity network. The OT-CMF provides a structured approach to baseline current capabilities, establishing a foundation for consistent evaluation and growth planning. It allows an organization to see the whole OT system. It is also a management tool for transit agency leadership to identify opportunities for growth, investment and evolution. Maturity does not come from spending the most money or implementing the most tools. Even at the lowest levels of maturity, many agencies need to orchestrate OT management to deploy a successful program.

2.3 Transit system standardization

This document is designed to be a companion to the OT-CMF Chart (Appendix A) the OT-CMF Controls Guidance (Appendix B) and the OT-CMF Implementation Guidance. The goal of this guide is to make it easier to start an OT security program and then mature it over time. The OT-CMF is a "framework" allowing a flexible application of cybersecurity best practices for OT. The OT-CMF is part of a systematic effort to reduce cybersecurity risk at transit agencies and will provide a roadmap for agencies to develop effective OT cybersecurity programs, as well as organize current OT risk management activities. The OT-CMF creates direction on aligning cybersecurity program efforts. These attributes include guidance to perform a baseline risk assessment; develop a documentation process; understand system weaknesses; and implement targeted training, continuous monitoring, incident response and improvement measures.

By using the OT-CMF, transit agencies will mature their security programs gradually and have an ability to measure cybersecurity maturity against other transit agencies. This move toward best practice adoption and standardization will establish consistency across transit agencies, providing them with a robust feedback process for lessons learned from the transportation sector and other critical infrastructure systems.

This recommended practice takes into consideration the unique mission/business requirements found in most OT environments (with a focus on the idea that most OT systems are commonly managed as part of the IT infrastructure). This OT-CMF should enhance best-practice discussions as agencies begin to work through understanding the boundaries of the OT environment and as conversation about resiliency evolve.

2.3.1 U.S. government expectations

In 2021, DHS issued TSA Security Directive 1582-21-01, "Enhancing Public Transportation and Passenger Railroad Cybersecurity." The SD requires agencies to:

- Designate a cybersecurity coordinator who is required to be available to TSA, DHS and CISA at all times (all hours/all days) to coordinate implementation of cybersecurity practices and management of security incidents, and serve as a principal point of contact with TSA and CISA for cybersecurity-related matters.
- Report cybersecurity incidents to CISA.
- Develop a Cybersecurity Incident Response Plan to reduce the risk of operational disruption should information and/or operational technology systems be affected by a cybersecurity incident.
- Conduct a cybersecurity vulnerability assessment using the form provided by TSA and submit the form to TSA. The vulnerability assessment will assess current practices and activities to address cybersecurity risks to information and operational technology systems, identify gaps in current cybersecurity measures, and identify remediation measures and a plan for the owner/operator to implement the remediation measures to address any identified vulnerabilities and gaps.

To provide a description of the incident's impact or potential impact on IT and OT systems and operations requires technical capabilities that many agencies still lack. Using the OT-CMF will guide agencies in developing the capacity to meet the spirit of the SD and future cybersecurity requirements.

The OT-CMF equips OT security professionals and leadership with adequate information and understanding to prioritize, align and pursue the most effective strategies to build an OT security program. Additionally, it assists transit agencies in maturing OT risk management practices at each level of their organization. The implementation of controls is highlighted, and directions are provided in Appendix B, further described in NIST 800-82 as well as outlined in the OT-CMF Implementation Guide.

The OT-CMF Controls Guidance will provide guidance on the following:

- selecting cybersecurity operational technology controls
- cybersecurity operational technology controls management
- implementing the operations of technology controls
- measuring the success of the operations technology controls
- achieving higher operations technology controls maturity levels

2.3.2 Important notes about system implementation

It is important to remember that most of the risk lies in the existing systems, which are many times harder to handle, as they're not under maintenance contract or they're just too old, and only the supplier knows how to deal with them. As agencies modernize and implement newer hardware, it is even more important to understand the security impact that new hardware and software components have on legacy systems, and vice versa.

Transit agencies should consider whether the proposed solutions are supported by the existing technology. This will include bandwidth, human resources requirements and capacity management. For instance, if proprietary technologies are involved, agencies must ensure that the value achieved by the implementation is greater than the costs of implementation. Secondly, silos exist in the organization, and even when an alert is raised it's not always clear which equipment the alert is emanating from or the system owner. This is troublesome as the alarm may be safety-related, and there may not be a playbook on how to respond.

3. OT-CMF Level 0

This level establishes the foundation necessary for developing, implementing, maintaining and maturing a cybersecurity program in a transit organization. It includes the following requirements.

3.1 Executive leadership provides a documented policy statement and commitment to supporting the development of a transit control system cybersecurity program

The vision of the agency's leadership and the communication of that vision to stakeholders is critical to launching an OT security program. Statements and policies from leadership affect all business groups at the agency. The commitment to a security program begins at the top. Senior management must demonstrate a clear commitment to OT security. OT security is an agency responsibility shared by all members of the enterprise and especially by leading members of the control system, safety and physical management teams. OT security programs with adequate funding and visible, top-level support from agency leaders are more likely to achieve compliance, function more smoothly and have greater success than programs that lack that support.

The development of an OT cybersecurity program will include the creation of agency policies. Therefore, supportive leadership is essential to success implementation. The importance of a policy statement cannot be overstated. It will guide the agency down a road to a sustainable program and can be expanded into a full-scale agency policy as the program develops.

To garner attention from leadership and business owners across the agency, the goals of the OT security program must align with the security vision, goals and objectives for the agency. This is important because, eventually, the characterization of systems and critical services that are dependent on OT will be foundational for developing organization-wide cybersecurity policies. Enterprise business systems and OT are different, and the special requirements for securing OT will become important. Most personnel in executive roles understand the threats to the IT environment. The nation has been discussing IT concerns for many years. The identification of nuances for the protection of OT, the patching of known security vulnerabilities and recovering systems after events (like ransomware) are a new subject area for them.

3.1.1 Initial outreach to agency leadership

Helping transit agency leadership understand the value of APTA standards such as network segmentation and NIST controls for OT will start the agency on a path to creating a transit control system cybersecurity program. However, leaders will not endorse a policy statement without a clear value proposition aligning the OT program and agency goals.

Leaders must be educated to understand that violating operational requirements while implementing security features in OT could cause more damage than a cyberattack. Most transit leaders will not want to move toward IT and OT systems as two programs. The cost will be the first consideration to a business leader who might not know the risk. The fact is that in transformations underway with mobility writ large, and among public transit systems specifically, the line between OT and IT is blurring. Transit leaders are attuned to cost savings and strategies to get more security for less money. This is being accomplished by sharing human resources and networks for IT and OT. They will need to be educated about the nuances in security OT and IT systems to launch the OT cybersecurity program.

Leadership must be presented with the risks related to *not* starting an OT security program. NIST suggests that this risk overview should be delivered in a three-tiered approach that addresses risk at the organization level, mission/business process level and information system level.

The support of leadership from the beginning of the OT maturity journey is critical. Most important is to get leadership to make the policy statement that everyone in the agency will adhere to the policy looking forward. That commitment will have two effects. First, it will make business unit system owners plan toward the spirit of the OT security policy statement. Second, it will allow the planning for further program development, providing a confidence that the agency's leaders will support OT security efforts, as well as build risk management programs inclusive of OT security requirements.

3.2 Identify a security champion with authority to drive the cybersecurity program

Even after leadership has defined OT security as an agency goal and issued a policy statement, a practitioner will be challenged to implement the many aspects of an OT security program alone. Depending on the level of the advocate in the agency or the role they play, a security champion will most likely be required to ensure continuous progress toward the OT cybersecurity program goal.

The security champion is vitally important because people in the agency will come to recognize this person as a trusted voice and authority. This security champion is most likely already a trusted advocate in the IT environment. Additionally, having this champion who is already known as a leader on some level to guide direction and strategy will help to eliminate ambiguity and confusion. This role is highly visible and prominent within the agency and requires a person who has a voice within the leadership structure. Their success will allow the agency to begin building a program that includes defining OT boundaries, performing assessments, analyzing potential impact and coordinating change management strategies with system owners.

3.2.1 Finding a security champion

Most practitioners in new cybersecurity programs "fall into" or are assigned the responsibility of developing a cybersecurity program, and some are brought in from the outside. They may already report to a specific department or arm of the organization (for example, IT). Their existing report-to executive may be the best choice for an executive champion because of their level of interest and ability to push the goals of the program forward, but this is not always the case. Here are some things to consider when soliciting an executive champion:

- How might the program be funded? What resources could be needed, and who controls those resources?
- Who is likely to be affected by the actions of the new program? How and to what degree?
- Who has expressed interest in the program and why?
- How do things get reviewed and approved at the agency? Who is involved, and what is their role?
- Based on an analysis of the organization, how does cybersecurity best align with the agency's needs, priorities and organizational structure? For example, is the need for the cybersecurity program more skills- and technology-focused (e.g., on system administration)? More safety- or security-focused (on directing or assessing people, policy and operations)? Both? And to what degree?

Soliciting feedback from other organizations or researching frameworks found in white papers and publications can help frame the thinking around where the program is best situated within an agency's organizational structure. This may or may not influence the report-to chain—by looking at what has worked for others and generic strategic advantages and disadvantages.

3.3 Identify and document operational technology assets

OT assets must be identified and documented. A key component of this effort is to identify all assets involving critical services that the assets support. IT and OT assets can then be assigned to a category. Responsibility for this effort should be delegated to a person at a level appropriate for the critical services being considered.

After the agency develops an understanding of the services required to achieve its mission, it needs to gather as much information as possible about each asset. The assets are the raw materials that support services needed to operate. A service needs people, information, technology and facilities. OT assets include software, hardware, firmware and any physical OT interconnections. Technology assets can reside anywhere within an organization, and it is up to the organization to determine how it describes the technology assets.

A good starting point is at the system level before looking at the network device level. The agency should have aligned its critical services and critical systems to the goals and objectives at this point. The final asset list will comprise all OT assets; however, their priority will be determined by their relation to critical services.

Below are important activities to consider while identifying assets:

- Assign responsibility for identifying assets supporting critical services.
- Identify people assets.
- Identify information assets.
- Identify technology assets.
- Identify facility assets.

3.3.1 People

People assets are the vital staff who operate and monitor the organization's OT services. People who are internal to the organization (and sometimes people who are external) oversee executing processes and procedures to ensure that the services are achieving the organization's mission.

When identifying people assets, the organization should consider the vital role required for the successful operation of a service rather than the actual person in that role. It is suggested that each role contain a defined list of the functions or responsibilities required in the performance of that role.

3.3.2 Information

Information assets are any information or data, on any media, required for the successful operation of an organizational service. An information asset can also be the output or byproduct of a service. Information can range from a bit or byte, a file, or a document to the collective information stored in a system. The organization must determine the granularity with which it wants to define its information assets.

3.3.3 Technology

Technology assets include software, hardware, firmware and any physical interconnections. Technology assets can reside anywhere within an organization, and it is up to the organization to determine how it describes the technology assets. A good starting point would be at the network device level, where common network components such as routers, servers and switches can be identified. The organization could then move on to personal computing devices such as PCs, laptops and tablets. Identifying broad categories gives the organization a starting point for uniquely identifying all the devices within its infrastructure, as well as setting boundaries for controls management.

3.3.4 Facilities

Facility assets are any physical plant or substation that an organization relies on when delivering or performing a service. Facilities can be owned and controlled by the organization or be under the control of external business partners.

The information security team should define, inventory and categorize the applications and computer systems within the OT boundaries, as well as the networks within and interfacing to the OT. The focus should be on systems rather than just devices. Assets that use a routable protocol or are remotely accessible should be documented. The team should review and update the OT asset list annually and after asset additions or removal.

3.4 Identify and create an implementation plan for Tier 1 OT-CMF controls

The security controls selected, based on the security categorization of the OT, should be documented in the security plan to provide an overview of the security requirements for the OT security program. The document should also describe the security controls in place or planned for meeting security requirements. As a reminder, security controls are protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity and availability) specified for an information system. Safeguards may include security features; management constraints; personnel security; and security of physical structures, areas and devices.

3.4.1 Common controls and control implementation

NIST advises in NIST 800-82 Rev. 2 that security controls exist for malicious code detection, spam and spyware protection, and intrusion detection. Not all controls may be appropriate for all ICS applications. HVAC systems and smart elevators may use select controls, as an example. Controls can be utilized for

receiving security alerts and advisories, and the verification of security functions on the information system. In addition, there are controls to detect and protect against unauthorized changes to software and data; provide restrictions to data input and output; check for the accuracy, completeness and validity of data; and handle error conditions.

When identifying and establishing potential controls, it is important to remember that a control can often apply across multiple processes, systems and/or assets in multiple operating units throughout the enterprise. These controls are referred to as common controls. Common controls are those that, once implemented, provide a security function that is inheritable by other organizational systems and processes. Enterprise-level controls apply across the enterprise, while common controls can be implemented at various levels. Common controls are often at the enterprise level; however, individual business units can implement common controls, which would then apply to systems and processes within that business unit. Policies and procedures developed and implemented at the enterprise level could be common to an entire organization. However, for example, a policy developed by the Finance Department that mandates multifactor authentications for all financial applications is not an enterprise control but would be inheritable, and therefore common, by all applicable systems in the Finance Department. This same perspective applies to OT security controls.

The agency-wide OT security program plan supplements the individual security plans developed for each organizational information system. Together, the security plans for the individual OT systems and the information security program cover the totality of security controls employed by the organization. Implementing controls is only the beginning of the process, and every agency must continuously adjust, maintain or improve the implemented controls. This will assist the agency in successfully achieving a risk management strategy that exists to positively impact the survival of the agency. From the moment controls are implemented, the agency must test them to determine if they are adequate for the level of protection required to meet the established risk management objectives.

3.5 Develop a cybersecurity hygiene and awareness program

Cybersecurity hygiene is a necessary component for an agency's security and the overall health of its digital environment. There are a few root causes for many data breaches, including malware infections such as ransomware, security incidents, and known but unpatched vulnerabilities in software.

Implementing security hygiene practices—such as patching operating systems, applications, and firmware—can address root causes of OT system security failures. Cybersecurity hygiene will prevent many incidents from occurring by minimizing the attack surface and lowering the potential impact of incidents that occur. In other words, security hygiene practices make it harder for attackers to succeed and reduce the damage they can cause. Security hygiene is not easy with regards to OT. Despite widespread recognition that patching is effective and that attackers regularly exploit unpatched software, many organizations do not adequately patch.

3.5.1 OT security awareness at the agency

Everyone working in the OT environment must be informed about the differences between managing IT and OT security. Failing to fully help stakeholders understand the delicate nature of applying security patches and connecting OT systems will open any organization to operational system failure. Like personal hygiene, cybersecurity hygiene should start with the basic actions that are most likely to promote good health of the OT systems.

OT security has characteristics that differ from traditional information processing systems, although some characteristics of enterprise security and OT security are similar. Many of these differences stem from the fact that logic executing in ICS has a direct effect on the physical world. Some of these characteristics include significant risk to human health and safety and to the environment, as well as serious financial issues such as production losses, a negative impact to a nation's economy and compromise of proprietary information.

As many of the older OT systems at an agency were never meant to be networked, they require a security practice that recognizes that IT fixes do not always apply. To further complicate matters, an agency's threat landscape changes daily, and new variants of attacks on computer systems appear by the hour. The sheer number of security vulnerabilities in hardware, software and underlying protocols—and the dynamic threat environment—make it nearly impossible for most agencies to keep pace. A loss of a function in an OT system could occur from attacks on IT systems and inadvertently from attempts to apply a traditional IT remedy.

3.5.2 Creating a culture of cybersecurity

Good cybersecurity hygiene is a risk-reducing technique that also minimizes employee errors. The approach mitigates a lack of knowledge related to online exploits. Cybersecurity awareness training is a best practice for protecting passwords and not unknowingly providing an advisory access. Protection starts with providing employees and contractors the knowledge to observe and identify attempts to access systems. A lot of high-profile breaches have been initiated using employee negligence as the network entry point. The employee was not malicious but simply ignored the organization's guidance for maintaining digital security. In some cases, transit organizations will need to apply access controls and limit connectivity to ensure compliance by employees and contractors.

Simply put, a transit agency needs to ensure that no one can interfere with its normal and proper operation. It should control what is going on and who has access, as well as the privilege to monitor and react to changing conditions. It is a best practice to start from the assumption that all login access is denied until a valid reason is given, and then the least amount of privilege is given to the smallest number of people. This practice is known as the "principle of least privilege." However, these concepts are implemented, they must also be shared with the internal and external stakeholders who assign duties to staff.

Training and organizational requirements are plentiful in some organizations, but how to apply and use resources is often missing. Training materials are typically full of regulations and technical terms. This is like a foreign language for the everyday user. However, the agency's security is dependent on users understanding their responsibilities.

The best approach to OT cybersecurity hygiene begins with activities that make stakeholders aware of the sensitivity of OT systems. A strong second step is to identify all systems and system owners. This will help in defining the environment to begin informally creating visibility of system OT–related activities. Not only do threats need to be shared across the organization, but changes in procedures and policies must also be communicated. Standards for good cybersecurity hygiene are about the people in the environment stressing to their peers how important the OT systems are to other critical systems. Each agency should teach the "See something, say something" rule. If something just doesn't seem right about the OT system, employees should tell someone, even if they are not sure about the exact nature of the issue.

3.6 Create awareness of known cybersecurity threats across the organization

DHS CISA has announced a significant trend it is seeing across critical infrastructure environments. Although there are very sophisticated hackers and powerful nation-state criminals attacking government and private sector entities, many of the successful attacks are using known threat vectors, many with patches and controls, to gain unauthorized access to networks.

Critical infrastructure entities are doing a poor job of sharing vulnerability and cyberthreat information internally. One of the challenging issues is ineffective sharing of information within business units and across the agency. Many of these agencies are making good use of well-crafted guidance they receive from government and vendors to resolve enterprise system vulnerabilities. However, the information received related to OT systems is not being optimally utilized to improve resilience of the agency. The threat to OT systems is not as well-understood and, in some cases, requires interaction and coordination between engineers

and cybersecurity personnel to turn external information into actionable intelligence to reduce risk to OT systems.

As an example, the cybersecurity analyst receiving information from external sources might not know that an OT vulnerability they received relates to a sensor's behavior for a specific OT asset. The issue could be specific to the asset or based on networking that equipment in a specific manner. If there is not a system of communicating with the system owner (who is most probably an engineer), that information identifying the vulnerability may not be communicated to the system owner. Over time, vulnerabilities that are manageable, but not managed, may accumulate. Therefore, it is critical that agencies begin crafting a situational awareness strategy.

Situational awareness provides an organization an understanding of its critical service's operating environment and the environment's impact on the operation of the critical service. This understanding in turn provides stakeholders with a sufficiently accurate and up-to-date understanding of the past, current and projected future state of a critical service. This supports effective decision-making in the context of a common operating environment.

It is critical that engineers responsible for managing and securing the OT assets assist the enterprise cybersecurity professional to understand the importance of information sharing and the type of information that is critical to managing OT vulnerabilities. It is just as important that the cybersecurity professionals or IT administrators share information with the OT engineers and let the engineers assess the value of the information.

Transit agencies will improve their ability to deliver information and cybersecurity awareness to the right custodian with a little practice. Trying is important. Each iteration should be based on input from stakeholders. Changes to the approach may come because of a need for cleared terminology, frequency, depth and relevance.

As information sharing begins and increases, agencies should already be considering situational awareness processes as needed to ensure that in the future:

- the process is a planned and coordinated activity between security and the business unit asset owners;
- process planning is driven by managing and mitigating organizational as well as technical risk;
- internal and external dependencies affecting cybersecurity awareness are identified and considered;
- there is an awareness roadmap that includes plans to one day have an organizational plan and measure the effectiveness of the plan;
- actions requiring management involvement are elevated in a timely manner;
- the performance of process activities is being monitored and regularly reported;
- key measures are within acceptable ranges as demonstrated in governance dashboards or reports; and
- actions resulting from internal and external audits are being closed in a timely manner.

3.7 Perform a cybersecurity self-assessment

Preparing and executing on a self-assessment can provide a valuable gauge of what is being done and the alignment with NIST and OT-CMF best practices. In the early stages of developing an OT security program, there will be a lot of best practices and activities that have not been implemented in an agency's environment. The self-assessment can reduce the cost of building a program and assist agencies in efforts to prioritize steps to build foundations for a successful program. Agencies typically will not need procurement approval since this activity is being performed in-house. Therefore, tools like the self-assessment are valuable to provide a common source for communicating where the agency is and updating requirements for where it needs to be.

3.7.1 Value of an OT self-assessment

The self-assessment provides an opportunity to understand the agency's alignment with NIST and APTA best practices for OT security. This activity will also help document the collective protection and sustainment requirements of associated assets.

One goal of this self-assessment exercise is to understand the OT boundaries. This effort begins a process for understanding the confidentiality, integrity and availability requirements of the service being used to derive the collective protection and sustainment requirements of the associated assets. It will also validate whether the assets put on the OT asset list are a complete set according to the established boundary, as well as the critical services being supported.

Activities that implement protection and sustainment requirements often appear as processes, procedures, policies, controls and plans. The OT self-assessment will allow an organization to identify protection requirements and identify how an asset's exposure to sources of disruption can subject the organization to exploitation of vulnerabilities. Examples of data derived from performing a self-assessment include the following:

- **People:** An understanding of the capabilities of staff members who are responsible for OT security to protect against accidental and adversary disruption.
- **Information:** How policy is being implemented for the protection of OT assets and whether new policy is required to prevent unintentional disclosure.
- **Technology:** Identifying whether network boundaries are adequately protected using approved methods and tools to deny unauthorized access. This is the first step to understanding how and where to implement controls.
- **Facilities:** Identifying whether physical access to all service-related information and technology assets is limited to approved personnel. The self-assessment will assist the assessor in understanding how an asset's exposure to sources of disruption and to the exploitation of vulnerabilities must be minimized.

In the end, this self-assessment serves two purposes: It helps with making a case for an OT security program, and it begins the process of understanding the OT system's vulnerabilities, threats and consequences. As the agency matures its OT program, the type and complexity of the assessment will also mature. Self-assessments are critical to agencies with limited resources. However, even as the agency incorporates external assessment into the risk management program, it should still implement a regiment of self-assessments.

4. OT-CMF Level 1: Initiated

This level builds upon Level 0 as a next step for enhancing, maturing and maintaining a cybersecurity program in an organization. Attaining Level 1: Initiate requires organizations to take the steps listed in this section.

4.1 Obtain formal acknowledgment and approval of the adoption of the OT-CMF from executive leadership

Obtaining support from management is essential to ensuring that the OT program is effectively implemented. A top-down approach often helps the program to meet the resilience objectives of the agency. A top-down approach also enables a consistent methodology for OT security programming and policies that will be implemented across the agency's boundaries. The level of management support required depends on where the OT program resides within the transit agency. Management will need to demonstrate support of the OT-CMF by providing appropriate funding, oversight and staffing. Support at the senior executive level is necessary to ensure the resilience of the program.

The security champion and implementers should now obtain formal acknowledgment and approval of the adoption of the OT-CMF from executive leadership. There are a host of security frameworks that can be used for assessments. There are no leading frameworks for understanding an agency's OT maturity. The OT-CMF helps to create standardization across the transportation sector and a path forward for OT-CMF program development. Smaller implementations, such as those at a small agency, may require sponsorship only from the management responsible for a particular service.

Agencies that do not use OT and run on an expanded enterprise network may reduce vulnerabilities with replacements of large percentages of their systems (in three- to five-year windows). Larger transit agencies are not able to minimize vulnerabilities in their systems by changing technology in this same way. The technology life cycle for enterprise cybersecurity products is much shorter than with OT. New systems often account for known threats to the hardware and software. Older transit systems rarely replace all their OT assets and are forced to manage known vulnerabilities for assets in use for longer than 30 years. Adversaries are familiar with these vulnerabilities and will exploit them when the opportunity presents itself.

Efficiently addressing OT cybersecurity issues requires a clear understanding of the current security state, emerging security challenges and specific defensive countermeasures. The OT-CMF affords a holistic approach—one that uses specific strategies for selecting and implementing countermeasures applied in layers to create an aggregated, risk-based security posture. This approach helps to defend against cybersecurity threats and vulnerabilities that could affect critical systems.

Agency leadership must be educated that, unfortunately, there are no shortcuts, simple solutions or "silver bullet" implementations to solve cybersecurity vulnerabilities within critical ICS infrastructure. It requires a multilayered approach. Maturing the program requires a focused approach to building capacity and capabilities in the OT program. The OT-CMF provides the approach transit agencies can voluntarily implement and move to higher levels of maturity at their pace.

See **Figure 2**.

FIGURE 2
Comparison of Enterprise IT with Industrial Control Systems

SECURITY TOPIC	INFORMATION TECHNOLOGY (IT)	CONTROL SYSTEMS (ICS)
Antivirus and Mobile Code	Very common; easily deployed and updated	Can be very difficult due to impact on ICS; legacy systems cannot be fixed
Patch Management	Easily defined; enterprise wide remote and automated	Very long runway to successful patch install; OEM specific; may impact performance
Technology Support Lifetime (Outsourcing)	2-3 years; multiple vendors; ubiquitous upgrades	10-20 years; same vendor
Cyber security Testing and Audit (Methods)	Use modern methods	Testing has to be tuned to system; modern methods inappropriate for ICS; fragile equipment breaks
Change Management	Regular and scheduled; aligned with minimum-use periods	Strategic scheduling; non trivial process due to impact
Asset Classification	Common practice and done annually; results drive cyber security expenditure	Only performed when obligated; critical asset protection associated with budget costs
Incident Response and Forensics	Easily developed and deployed; some regulatory requirements; embedded in technology	Uncommon beyond system resumption activities; no forensics beyond event re-creation
Physical and Environmental Security	Poor (office systems) to excellent (critical operations systems)	Excellent (operations centers; guards, gates, guns)
Secure Systems Development	Integral part of development process	Usually not an integral part of systems development
Security Compliance	Limited regulatory oversight	Specific regulatory guidance (some sectors)

NOTE: Compare the business/enterprise point of view (middle column) with the industrial control system (right column).

4.2 Appoint security liaisons across the organization to coordinate cybersecurity program activities in their respective business units

As NIST has described the requirement for a senior agency-wide security officer, different levels (business roles) of the agency should eventually appoint individuals to a security role with responsibilities within business units. The responsible parties for the OT environment should appoint a knowledgeable person with the mission and capability to coordinate, develop, implement and maintain a department's security program. The person will work in close coordination with officials like a chief information security officer. Clear reporting procedures should be established to ensure few deviations from the stated risk tolerance at each level of the agency.

The security champion is the key to assisting the agency in meeting its security goals. The business unit representatives will look to the champion as a knowledgeable official who is carrying out the goals of the agency. Agencies are most secure when all business units are collaborating and following a set of policies

aligned with the security goals, objectives and guidelines for the entire agency. There may be security liaisons in several business units depending on the size of the agency. The more liaisons there are, the more important it is to have coordination and collaboration. Agency-wide cooperation will lead to faster gathering of information for executive decision-making.

4.2.1 Identify agency liaisons

The analysis of the agency's vision, mission and culture will probably produce some idea of who the program stakeholders might be, but it is best to do more structured analysis. For first-time program development, security professionals should consider speculating on what they think they might need or produce from the cybersecurity program at a very high level, and who would supply or consume those inputs or outputs. These people may become the security liaisons across the agency.

A useful tool for identifying stakeholders is SIPOC, which stands for "suppliers, inputs, processes, outputs and customers." This is a five-step methodology for identifying stakeholders who contribute inputs to, or consume outputs of, a business process. The steps are to identify the following:

- the process (parts)
- process outputs
- consumers of those outputs (customers)
- prerequisites for the process (inputs)
- who supplies those inputs

The full SIPOC method can be used again as cybersecurity projects and initiatives are developed and the processes and players change. The results of SIPOC can be mapped to a grid. **Table 1** is an example of a modified SIPOC analysis for a new cybersecurity program.

> **CAUTION:** Each agency is different; the groups and individuals identified as stakeholders should map to the agency's own organizational structure and what was learned through the research on its strategic priorities and culture. The inputs and outputs may vary based on how the agency delegates authority, divides resources, addresses tasks and consumes information.

TABLE 1
SIPOC Analysis for a Cybersecurity Program

Suppliers	Inputs (Needs)	Process	Outputs (Products)	Customers
• CFO (budget) • CIO (IT manager) • Materials management (procurement of goods and services) • CSO (safety/security) • Vendor partners (e.g., MSSP) • IT administrator	• Funding • System admins • RFP/supplier management • Managerial authority • Staff with specific skills	• The cybersecurity program	• Policies and procedures • Compliance reports (gap analysis) • Trend or progress reports • Risk register	• Computer users (multiple departments) • Computer administrators (IT) • Operations teams (control systems) • Auditors • GM/board of directors

4.2.1.1 Getting to know stakeholders

Once a pool of prospective stakeholders has been identified, it's important to meet with each of them to understand their perspectives (if not already done during the earlier research). Consider the following questions:

- What motivates them?
- What do they want or need from the program or the security professional?
- What are they most interested in, related to the program or related to the agency?
- What could the program contribute to them?
- What is their relationship with others within the agency (e.g., trusted staff or allies)?

Most transit agencies are people-focused organizations. Despite the existence of conferencing technologies, if it is at all feasible, it is imperative to meet stakeholders face to face, in their place of employment. This will allow them to show the security professional what they are excited about and provide an opportunity to learn, observe and think about how the cybersecurity program could contribute to that person or their department's goals—or benefit from their help.

4.3 Define and approve the purpose of each operational technology asset

Agencies at Level 0 start the process of identifying assets. Level 1 is the time to review them and understand their purpose. Cyberattacks may exploit and target specific system layers within the transit agency, including but not limited to OT systems. Unnecessary assets hanging on a network can create a threat vector.

A transit agency must know if its vendor will support patched versions of the applications, and it must also know the vulnerabilities that will exist if it does nothing. In general, if the application is for convenience or is not required, then it should either be removed or locked down so an attacker cannot use it as an entry or control point. If the application controls a critical function, then the purchase should be assessed to understand the overall risk to the organization.

Over time, systems integrating SCADA, original equipment manufacturer and other critical component technologies responsible for the control, movement and monitoring of transportation equipment and services can accumulate a large collection of assets. Often such systems are interrelated into multimodal systems such as buses, ferries and metro modes. Assets can very easily go unnoticed and unmanaged, especially if they are in remote locations. Therefore, it is important to map assets to the critical services the assets support. It is also important to associate assets to safety and security zones. This concept is further discussed in the APTA OT-CMF Implementation Guide. Initiating a system development life cycle (SDLC) process is a methodology to manage the assets as well as to ensure that all are accounted for within a transit environment.

4.3.1 System development life cycle (SDLC)

It is critical to understand what is in the network and what the asset's purpose is to the operations of the agency. By utilizing the SDLC process, transit agencies can more effectively manage the security of technology environments. Many SDLC models have been developed, but they generally cover five major phases:

- Initiation
- Development/acquisition
- Implementation
- Operations/maintenance
- Disposal

With the goal of maintaining information security through maintaining confidentiality, preserving integrity and sustaining availability, transit agencies must integrate security in each of the phases in the SDLC. Utilizing security activities outlined within each phase developed by NIST SP 800-100, transit agencies will have a broad understanding of the security activities necessary within the SDLC process. In 2021, NIST released NISTIR 8397, "Guidelines on Minimum Standards for Developer Verification of Software." The document recommends minimum standards of software verification by software producers. However, buyers can use the recommendations to improve acquisition language for suppliers who provide software products.

A common misconception is that OT and SCADA systems are not vulnerable to cybersecurity attacks given that such systems are not directly linked to the internet and typically do not have a graphical user interface (GUI). While it is true that early OT systems were designed and built on separate networks and controls, advancements in IT infrastructure and the evolution of information management practices required the link between OT and enterprise systems. However, methods to exploit security vulnerabilities and gaps of specific OT systems are documented by CISA as well as by many underground hacking organizations and individuals. Reviewing and managing all assets allows agencies to reduce threat vectors. Taking unnecessary assets off the network provides better security through an up-to-date mapping of the network architecture.

4.4 Collaborate with business groups/units across the organization to document security operating procedures and processes

The enterprise IT systems help professionals to collect, store and manage information at transit agencies. The OT systems help those same agencies to monitor and make systems work across the enterprise. The more an enterprise relies on technology of any kind, the more vulnerable and susceptible it becomes to suffering a severe security breach. Coordination and collaboration with the people closest to the OT procedure and processes will be critical to keeping systems, human errors, hacker attacks and system malfunctions at a minimal level. All the previously mentioned faults are issues that occur when the procedures and processes are not complete. It is critical to not just produce processes and procedures, but also to validate the directions in the documents. Hence, practitioners and system owners must be instrumental in the creation of the processes and procedures.

The scope and hierarchical relationship among policies and procedures needs to be managed for maximum effectiveness. Agencies should implement cybersecurity policies to set a tone for how the organization will access risk, manage the life cycle of systems, and respond to incidents. These policies outline guidelines and provisions for preserving the security of data, software and technology infrastructure. The agency operating procedures are the directives for the procedures and processes the OT professionals will be responsible to manage and keep updated.

The value of working in an inclusive manner cannot be overstated. These people will have experience and understand the business unit culture in a way that can enhance any practice that is proposed. They will also understand the consequences of not having a standardized approach to OT security. The insights and experience can be an opportunity to tweak proposed guidelines and directions.

Vulnerabilities and predisposing conditions are often introduced into the ICS because of incomplete, inappropriate or nonexistent security policy, including its documentation, implementation guides (e.g., procedures) and enforcement. Management support of security policy and procedures is the cornerstone of any security program. An agency's security policy can reduce vulnerabilities by mandating and enforcing proper conduct. Written processes and procedures are mechanisms for informing staff and stakeholders of decisions about behavior that is beneficial to the agency. From this perspective, policy is an educational and instructive way to reduce vulnerabilities. Enforcement is partner to policy, encouraging people to do the "right" thing. By collaborating at the onset of process and procedure, everyone understands the importance of

the practice to the agency. Additionally, team members are less likely to push back on the processes and procedures.

For many of the reasons stated, processes and procedures can't be produced in a vacuum. The people closest to the system must be a part of creating the practices they will support and are expected to follow. In some cases, these team members will know the situations within a specific agency that require creating an extra step or work-around to enhance the process or procedure. They should not be doing things outside of the final process or procedure. Thus, it is critical that they be a part of creating it.

When it comes to the policies that the processes and procedures are modeled after, there is usually a complex compliance environment that includes laws and regulations, overlapping jurisdictions and spheres of influence, economics, custom, and history that have a significant influence. By creating an inclusive environment, it is an opportunity to teach and define the challenges the agency is attempting to overcome. A well-written procedure will consider the responsibilities of individuals from different organizational units and the relationships among them.

4.5 Publicize known cybersecurity threats across the organization

A very important aspect of building a culture of cybersecurity at a transit agency is helping team members to understand the cyberthreats the organization faces. Communicating accurate information in a timely manner to relevant stakeholders is essential for good decision-making and allows stakeholders to take appropriate actions that prevent or mitigate risks to critical services.

The way the information is presented to stakeholders is a key aspect of supporting good decision-making in the face of a dynamic risk environment. Using situational awareness data to support decision-making involves careful consideration about what information to present, when to present it, to whom to present it and in what form. Attempting to present all available situational awareness information to all stakeholders in a timely manner is almost always counterproductive, if not impossible.

For rapid and effective decision-making, different stakeholders typically need different views or slices of the common operating picture (COP) that are customized for each class of stakeholder and consider characteristics such as the level of abstraction of the information presented, the focus and context of any alerts or alarms, the sensitivity of the information with respect to any associated security requirements (i.e., for the confidentiality, integrity and availability of the data), and the form or format of the data (for human or machine consumption).

Unlike cybersecurity skills training, awareness efforts communicate a message to a broad group of employees with different skills and experience. The awareness message often conveys information about organizational goals, objectives and critical success factors. The message can also provide employees with information that improves operational resilience (e.g., security and confidentiality guidelines, vulnerability alerts, and incident notices). Awareness needs are identified through multiple sources, such as the following:

- resilience requirements
- organizational policies
- vulnerabilities under watch
- laws and regulations
- service continuity plans

In addition, plans for domain processes can be reviewed for awareness activities needed to provide staff members with an understanding of the organization's cybersecurity resilience concerns. Another way to

gather awareness needs information is to interview managers responsible for the different aspects of the organization's cybersecurity resilience efforts.

By providing information about known vulnerabilities, the agency makes cybersecurity everyone's responsibility. It is also useful to identify different groups of people by the types of awareness information they need. For example, the general population of an organization may need information about organizational goals and objectives, and those responsible for responding to a service disruption will need information on changes to service continuity plans.

Documenting and accumulating awareness needs across the organization provides an overall picture of the extent of awareness activities to be conducted, as well as the different awareness categories (such as personnel groups or need for urgency). The threat information creates a sense of alert for stakeholders. Once they are aware of the threats, it provides them an opportunity to put their cybersecurity awareness training to good use. Therefore, good cybersecurity hygiene training that supports each role at the agency should be paired with plans to share the threat information. Make the information as usable as possible, and continuously communicate with stakeholders to understand how they used the threat information in their environments.

4.6 Building and using a test environment

NIST instructs organizations to develop a test environment as part of the security infrastructure. It is critically important to know how patches and system updates will impact the function of OT systems. Agencies will patch and structure system maintenance based on their abilities to support patching requirements and the controls selected. Software patches should be tested on a sandboxed or isolated system (test environment). A sandboxed system is a test system to reproduce or actualize an operation in an isolated environment. It provides an opportunity to "fail" without impacting a production system, as well as helps agencies uncover malicious code in a safe environment.

Due to the costs, some agencies will not build a test bed or replicate their network architecture. When a test bed is not available, security professionals should ensure that the organization is intentional about using safe patching practices. This also applies to activities focused on implementing new technologies in live or production systems. The organization should be prepared for potential network or system impact with the introduction of both software and hardware. A detailed OT recovery plan must be in place with trained professionals ready to implement a system recovery strategy.

Agencies should consider that different levels, tiers or zones in the transit network may have different maintenance requirements. The APTA zones have different significance and importance depending on the agency's architecture, boundaries and critical zones. Planning is critical to managing change, the required maintenance and desired growth in transit networks.

4.7 Implement a cybersecurity hygiene and awareness program

Training and awareness efforts for OT typically take place at various levels of an organization. The training program for the entire agency addresses agency-wide needs. Specific training and awareness activities for OT are typically developed and implemented at the business unit or team level where they are needed. For training and awareness at any level of the agency, management support is essential. With management support, processes are defined to identify, implement and assess training and awareness on an ongoing basis to ensure enough skilled employees to provide resilient services.

Planning for training and awareness is essential for a successful OT program. There should be a plan developed that aligns with the agency's training objectives. The plan will document the program objectives, a strategy for achieving those objectives, and the infrastructure and resources needed to execute the plan.

Important activities while planning for training and awareness activities include the following:

- Obtain support for training and awareness planning.
- Establish a training and awareness program strategy.
- Establish an approach to building a training capability.
- Establish an approach to building an awareness capability.

Conducting OT training and awareness activities usually involves engaging multiple levels of the organization, as well as third-party providers. Cybersecurity resilience efforts should be incorporated into any existing training and awareness program and evaluated for effectiveness.

4.7.1 OT training and awareness considerations

It will be easy for the uninformed planner to overlook the nuances of OT security. Establishing capability for cybersecurity resilience training and awareness includes identifying and developing the program's educational vehicles (courses, presentations, etc.). Each organization will have unique needs for cybersecurity resilience training and awareness that must be addressed with activities developed specifically for the organization, as well as common needs that can be met by third-party providers. All training should improve the resilience of the agency and provide a platform to build from as the agency grows its OT cybersecurity program.

Important activities for building capability and conducting training and awareness include the following:

- Establish and maintain support functions for training and awareness (e.g., library for storing materials and a record tracking system).
- Develop training and awareness materials.
- Procure third-party provider services.
- Conduct training and awareness activities.
- Improve training and awareness capability.

In the evaluation and improvement phase of the training and awareness process, the organization should evaluate training and awareness activities against the agency's objectives. If the activities are not meeting their objectives, then the agency must initiate improvement actions. Improvements to the training and awareness activities, based on the analysis of the collected data, should support the achievement of the agency's objectives.

To be effective, OT training and awareness activities must be meaningful to both the employee and the agency. Evaluators must plan accordingly to collect sufficient data to examine the effectiveness of the activities and recommend improvements to be incorporated in the next cycle. The data collected should allow the analysis of the programs against four desired outcomes:

- Employees are better able to perform their jobs.
- Supervisors are better able to assess changes to their employees' on-the-job performance.
- The organization feels confident that the employees are performing activities in a way that demonstrates a resilient organization (e.g., meets the goals and objectives).
- The training and awareness activities can be improved.

Evaluation requires the collection of data and observations throughout the organization's training cycle. Evaluation and analysis of training and awareness programs should occur at an agency-defined frequency to support the incorporation of updated material and synchronization with the execution of the training and awareness plan.

Important activities in the training and awareness assessment process include the following:

- Establish a plan to evaluate the training and awareness program.
- Evaluate the training and awareness program and analyze results.
- Improve the process.
- Update training and awareness materials.

4.8 Revise and republish the approved procedures and processes to relevant stakeholders

The identification of risks is a foundational OT risk management activity. A transit agency will have difficulty successfully managing its risks if it does not understand what they are. Agencies need to ensure that they have the capability to identify risks in a timely manner and then communicate those risks to the appropriate stakeholders. With the identification of risk and risk mitigations, the policies and procedures for a given practice may change. These adjustments as to how the risk is managed should be documented, approved by relevant business units' leadership and shared with all appropriate stakeholders.

Typically, agencies struggle with communication. This may become more obvious as the transit agency grows. Whereas verbal communication in meetings ensures that stakeholders heard a message about procedure and process change, undocumented changes, as well as documented changes outside of face-to-face interaction, create challenges in some organizations. First, the information may not be delivered adequately, and second, a relevant stakeholder who has mastered the communications may change roles. Therefore, previously discussed processes to identify people assets associated with critical services and manage the information is very important.

4.8.1 The communication process

The communication process refers to a series of actions or steps taken to successfully convey a message to the appropriate team. It involves several components, such as the sender of the communication, the actual message being sent, the encoding of the message, the receiver and the decoding of the message. There are also various channels of communication to consider within the communication process. This refers to the way a message is sent. This can be through various mediums such as voice, audio, video, email or fax. The overall goal of the communication process is to present an individual or party with information and have them understand it. The sender must choose the most appropriate medium for the communication process to work successfully. Whatever method communications are delivered in, they must reach the right recipients.

It is as critical that processes and procedures are properly communicated as it is to document them. The communication process is an organizational flaw that hackers readily exploit. How many times after an event has someone said, "Well, no one ever told me we changed the procedure."

The lack of communication about changes in processes and procedures can also have legal, regulatory and safety implications. For example, a change made for a mechanical reason could cause the loss of life if the person was not informed in a timely manner. The consequences of not communicating changes appropriately to relevant stakeholders would then become a reputation and financial liability.

The communication process has several components that enable the transmission of a message. Here are the various parts:

- **Sender:** This is the person who is delivering a message to a recipient. Changes in policies and procedures should be delivered from an authority figure in the organization like the OT security champion. This will help to emphasize the importance of the message.

- **Message:** This refers to the information the sender is relaying to the receiver. The information must be provided in a way that signifies its importance. In a busy OT environment, it will be easy to put some communications on the back burner when practitioners are focused on protecting the network.
- **Channel of communication:** This is the transmission or method of delivering the message. For agencies with a dispersed population of stakeholders, the delivery method may be different than in situations where stakeholders are collocated.
- **Decoding:** This is the interpretation of the message. Decoding is performed by the receiver, and over time agencies will learn how to best deliver updates. It is important that changes in policies and procedures are understood. To achieve this goal, the agency may need to provide some training or workshops to relevant stakeholders.
- **Receiver:** The receiver is the person who is getting the message. The communications must be phrased, translated or simply explained in a way to get the expected action from the receiver. The bottom line is that if the people expected to carry out the agency's policies and procedures don't understand them, the probability that the agency's goals will be achieved is low.
- **Feedback:** In some instances, the receiver might have feedback or a response for the sender. This starts an interaction. For OT security this is important, because an asset custodian may have a critical input that will again cause a change in the policies and procedures. The processes must be interactive.

4.9 Review the recommended OT-CMF controls, and perform a cybersecurity self-assessment on an annual basis

Every agency should perform a review of the recommended OT-CMF controls. These controls can help to reach a desired state of OT security or capability at an agency when implemented. An example of security controls implementation might be if an agency wants to secure endpoints. Several controls can contribute to build this capability. When performing an assessment, the controls should be assessed for overlap and that the control closes the vulnerability that has been identified.

Reviewing the security of the OT network using security controls allows for a more consistent, comparable and repeatable approach to understand risks. Controls contribute to the breadth of an organization's understanding of its capabilities to manage cybersecurity risks. Some controls have a higher level of criticality, such as those that look at safety systems. Other controls are important but may relate to the operation of a noncritical system like public Wi-Fi access. An assessor needs to understand the totality of the network architecture, because in some cases an organization may be using the Wi-Fi for connection to a critical system.

The sequencing of control in an assessment may also help an assessor to better understand the systems being assessed. The construct of controls to create a capability helps to assess the severity of vulnerabilities discovered in a system. Ultimately, if there is a failure associated with a vulnerability, the agency should determine if it was a failure of a particular security control or privacy control. Assessors should be aware that control interaction may impact the overall security and contribute to the complexity of understanding the outcome of an assessment.

To take advantage of the expanded set of security and privacy controls, and to give organizations greater flexibility and agility in defending OT systems, the concept of overlays was introduced in the latest revision of NIST 800-53. Overlays provide a structured approach to help organizations tailor security control baselines and develop specialized security plans that can be applied to specific missions/business functions, environments of operation, and/or technologies. This specialization approach is important as the number of threat-driven controls and control enhancements in the catalog increases. Agencies must develop risk management strategies to address their specific protection needs within defined risk tolerances and objectives.

5. OT-CMF Level 2: Planned

This level builds upon Level 1 to further enhance and mature the organization's control system's cybersecurity program. Attaining Level 2: Planned requires organizations to take the steps listed in this section.

5.1 Obtain executive approval for establishing a charter, a Cybersecurity Governance Committee and the appointment of a committee leader

This document has discussed at length how executive leadership approval is important at different steps in the process. Support from leadership is critical to bringing a focus to the OT security requirements. It is important to get the program activities launched, but sustainability will come from establishing a charter, a Cybersecurity Governance Committee and the appointment of a committee leader. Executive leadership concurrence with the process and the authority of the committee and its goals provides the leverage to apply the OT cybersecurity program across the agency.

The Cybersecurity Governance Committee for OT will be important to how risk objectives, risk review and OT policy are defined. Although this committee will not have board of director authority, it will impact the information the board receives to make agency-wide decisions. The board will ultimately decide the authority and potentially the makeup of the committee. If the board is focused on the OT challenge this closely, the OT program has already tallied a win. Most likely, the committee will be launched by an executive officer with OT operations under their purview. In any case, the importance of the work will be the same.

The leader or chair of the governance committee is important, as they will work to lift the work of the committee and ensure that its work aligns with the goals and objectives of the agency.

The committee charter should do the following:

- Elaborate on the reason the committee exists in terms of its value and contribution to the agency's overall needs and wants.
- Identify the committee members, their roles and the importance of their roles on the committee.
- Set clear expectations for the committee members (i.e., identify what inputs they will give).
- Specify how the committee communicates (meetings, website, email, etc.) and how frequently.
- Identify outputs of the committee (what it hopes to achieve and what products it will manage). Among the first of these, the committee should address the program roadmap, including its development, refinement, and continual review and improvement.

5.2 Cybersecurity Governance Committee

The OT Cybersecurity Governance Committee has a host of functions. Among them are the responsibility to outline the security management structure and assigns security roles and responsibilities. Additionally, the committee should define control system's cybersecurity program goals and objectives according to the OT-CMF. Other responsibilities of the OT Cybersecurity Governance Committee are listed below.

5.2.1 Define the security liaison's roles and responsibilities in coordinating cybersecurity program development and dissemination activities within their business units

Business activities across an organization typically take priority. Cybersecurity is a support function for ensuring the confidentiality, integrity and availability of critical services and assets. For the activities to support the business to flow unencumbered and meet the requirements outlined in policies, security liaisons must be guided by documented procedures. The Cybersecurity Governance Committee will align the liaisons

to support the strategies for risk management, situational awareness and incident response. The written guidance is important, as it also informs the leadership structure for the liaison of duties and responsibilities that must be carried out in support of agency resilience.

5.2.2 Develop agency-specific policies, procedures and processes

The OT-CMF provides guidance for the voluntary implementation of security practices to mature an OT cybersecurity program. The OT-CMF is designed to allow agencies an opportunity to frame policies, procedures and processes that align with the framework but that are specific to them. Agencies may recognize that they are performing practices at a higher maturity level than their assessment identifies. However, an agency has not reached a maturity level until it is performing all the activities at that level.

The Cybersecurity Governance Committee will assist an agency in defining that speed of maturity. The committee will also review the tasks at each tier to ensure that the requirement is being met and set goals to move the agency to the next level. The committee will be able to explain to the board of directors a suggested path, as well as inhibitors to maturing the OT program.

5.2.3 Define the cybersecurity policies and standards for procurement and acquisition

Critical cyber-assets such as SCADA systems, BMS, advanced metering infrastructure (AMI), and OT are found in critical transportation infrastructure. They can have unique software, firmware, application, vendor and communications protocols; however, the procurement requirements to ensure the confidentiality, integrity, authentication and availability share several similarities. Cybersecurity managers must work with procurement officials to ensure that acquisition requirements don't supersede the security and risk management objectives for the acquisition. When it comes to purchasing components, or systems or assets that connect components to create a system, details matter.

OT cybersecurity must be a part of the procurement process. The Cybersecurity Governance Committee will define and manage the requirements that help to ensure that those purchasing and supplying technologies consider cybersecurity from the design phase, which ensures that cybersecurity is implemented throughout the procurement life cycle. By implementing cybersecurity procurement and implementation guidelines, the committee can help to mitigate systems-level cyberthreats and expedite secure and sustainable deployment and integration of critical SCADA, smart systems and automation technology.

5.2.4 Develop an OT Risk Management Program and ensure that OT-CMF aligns with the Enterprise Risk Management Program

CISA advises that a cybersecurity awakening may drive a compelling need for change and push organizations to take an aggressive approach to implementing a new risk program. However, an overly aggressive approach can be problematic or too costly. There is often a steep learning curve for an organization as it matures its risk management capabilities. Organizations that are implementing a new risk management program can benefit from focusing on a few key tasks and establishing a goal of iteratively refining the program over time as staff gain experience and the organization deepens its resource investment in risk management. The Cybersecurity Governance Committee will be critical to guiding this effort and ensuring a leveled application of processes across the agency.

5.2.5 Identify key performance indicators and key risk indicators

The work of the Cybersecurity Governance Committee is critical to ensuring that the board of directors is never blindsided. One of the methods to achieve visibility and awareness of cybersecurity changes is to develop KPIs and KRIs. The KPIs will make it easier for the board to assess activities against baselines and investment. The KRIs will inform the board on actual risk versus the risk tolerance of the agency. These two

indicators allow a holistic view of performance and risk, as well as the risk-versus-reward questions the board of directors should be examining.

5.2.6 Collect and analyze risk data from all control systems to establish risk acceptance criteria

The Cybersecurity Governance Committee will define the policies that mandate specific collection methods; the analysis regimen; and the procedures following a suspected breach where artifacts and data are collected, analyzed and maintained. There are many methods of collecting risk data and analyzing it to establish risk acceptance criteria. The more data points, the greater an opportunity to identify potential deviation from risk goals, cybersecurity exploits and even general system performance. The agency must gain access to vulnerability, threat and consequence data to make the best decisions regarding risk disposition.

All the collection and analysis activities support the Cybersecurity Governance Committee being able to make sound decisions. If the committee determines that the organization is not able to make a risk calculation due to a lack of a risk component (vulnerability × threats × consequences), it should make decisions on adjustments to investments and training to obtain the data. The goal is to define repeatable processes that will create a culture of risk reduction.

If the data necessary to make risk decisions is available, the committee should be able to establish risk acceptance criteria. First, however, the committee should perform an exercise that examines costs associated with buying down risk, the agency's ability to manage risk and limitations on transferring risk.

5.2.7 Establish guidelines and benchmarks for measuring progress and compliance with the OT-CMF

The performance of the OT security system can be measured only if there are baselines and targets to measure against. The Cybersecurity Governance Committee will set the risk tolerance levels and determine acceptable practices to identify whether the security program is incompliance with the practices identified. The committee will also provide the strategy for implementing the OT-CMF and align the long- and short-term performance goals. Over time the committee will manage the adjustments to OT cybersecurity efforts to stay on target with the OT-CMF implementation plan.

5.2.8 Develop an organizational control system cybersecurity training and awareness program

An important aspect of "Protect" in the NIST Cybersecurity Framework is to develop and implement appropriate safeguards to ensure delivery of critical services. The Protect function supports the ability to limit or contain the impact of a potential cybersecurity event. Important to this capability is the training and awareness effort across the agency. The Cybersecurity Governance Committee should define the risk tolerance and the training and awareness requirements for the agency. It should also ensure that staff skill levels do not contribute to exceeding the risk tolerance. The committee is pivotal in ensuring that there is adequate funding to provide training on OT systems. Lastly, the committee will review the training program to make sure the proper evaluation of training regimens is occurring as planned.

Awareness and training are not the same. Many stakeholders in the agency will need to be aware of the OT systems and general differences from the IT systems. Most will not require role-based training, just reminders of their responsibilities and the threats to both IT and OT systems. The committee should spearhead efforts to build a culture of cybersecurity using awareness activities as a starting point.

5.2.9 Clearly define service level agreements/operations level agreements

The cybersecurity requirements for the acquisition process should be defined by the Cybersecurity Governance Committee. The committee should ensure that the agency adjusts the ICS procurement process to weigh cybersecurity heavily as part of the scoring and evaluation methodology. Additionally, the committee should ensure that the upfront investment secures ICS products, evaluating security against current and future threats over the projected product life span.

When a vendor or specific products are being procured, there should be a policy related to acceptable service level agreements. Products that will not receive vendor backing through downtime agreements or acceptable response times should incidents occur should not be purchased. DHS CISA advises that establishing contractual agreements for all outsourced services that ensure proper incident handling and reporting, security of interconnections, and remote access specifications and processes is key to managing external dependencies. The committee should consider ICS information integrity, security and confidentiality when contracting with a cloud service provider. The ability of the agency to gain visibility of its data when required is important. CISA suggests that agencies leverage test labs, when possible, to test vendor-provided software for malicious code and defects before implementation. And agencies should have recourse when products don't function as intended or promised.

5.3 Define and document the OT safety and security zone architecture

It is critically important to define and document the safety and security zone architecture. In transportation the most critical function is the protection of life and safety. However, it is not easy to implement system attributes that support this concept. Transit agencies must find a way to implement the security zones across this vast space, accounting for people, technology, information and facilities. This effort also requires controlling the physical access and permissions across the various physical locations. Even with these challenges, an agency should always start with the basics.

A transit agency should restrict each group (or division) to its own equipment and systems to reduce the chance of an innocent mistake becoming a serious problem. To make systems safe, it must be acknowledged that everyone is human. Mistakes are inevitable. A good system builds in controls, logging and other procedures to ensure that people do their jobs. All workers must be reminded when they are accessing critical equipment or systems and challenged when they try to enter sensitive or secure locations. They should have to show ID, use a special key, or enter a special value—such as a pass phrase or password—into a system before being able to make changes.

It should be a requirement within each agency that all devices connected to the internet be protected with a firewall. This isn't always possible, and in those cases, monitoring and mitigations should be in place to identify intrusion and incidents. A firewall is a network security system that creates a buffer zone between the transit agency's network and external networks (see **Table 2**).

TABLE 2
List of Zones (APTA Enterprise Cybersecurity Working Group)

External Zone	The external zone includes internet-accessible services, remote operations and facilities, and remote business partners and vendors. It is *not* trusted.
Enterprise Zone	The enterprise zone, or corporate zone, includes, where applicable, hardware and services that are made available to the control system via the agency's corporate network, including agency business systems, fare collection systems, email, VPN, central authentication services, etc.

Cybersecurity protection of the three zones shown in **Table 3** is addressed by the APTA Control and Communications Security Working Group.

TABLE 3
List of Zones (APTA Control and Communications Security Working Group)

Operationally Critical Security Zone (OCSZ)	The OCSZ includes the centralized SCADA, general train control, communications-based train control, transit passenger information system, and other centralized control hardware and software, and the equipment from these control center zones extending out to remote facilities such as train stations and trackside equipment.
Fire and Life-Safety Security Zone (FLSZ)	The FLSZ contains any system whose primary function is to warn, protect or inform in an emergency.
Safety Critical Security Zone (SCSZ)	The SCSZ contains any system that if hacked and modified would cause an immediate threat to life or safety—for instance causing a collision or derailing a train.

For each function and system used by a transit agency, the agency should assign it to exactly one zone. Some functions are preassigned to a zone and may never be assigned to another zone. For other functions, an agency may choose the appropriate zone based upon the circumstances of its transit system. Ventilation systems, depending upon their purpose, may be assigned to either the OCSZ or the FLSZ. How does the agency choose? If the agency has only above-ground train or bus stations with no need for emergency ventilation, then it may assign ventilation systems to the OCSZ; if it has below-ground train stations, it should assign the emergency ventilation portion of the ventilation system to the FLSZ.

Vital rail signaling, interlocking and automatic train protection must always be in the SCSZ. For traction power in a station, controlling the power should be assigned to the OCSZ, while the traction power emergency cutoff (blue light) system and protective relaying should be assigned to the FLSZ. These systems may never be in the Enterprise Zone, External Zone or SCSZ.

5.4 Implement agency-selected Tier 2 OT-CMF controls from Level 1

Each agency will select security controls that are best suited for their environment and that align with agency goals. Consult the OT-CMF Controls Guide (Appendix B) to select Tier 2 OT-CMF controls.

5.5 Assess and select Tier 3 OT-CMF controls to be implemented in Level 3

As agencies mature and move from one maturity level to the next, they should assess their security requirements. Security controls may change with the addition of new processes and technologies. The adjustments of agency goals and objectives may also impact the controls. Therefore, prior to moving to the next maturity level, an agency should review existing controls, risk and vulnerability assessments, and the target risk tolerance to assess the need for refinement or addition of new controls.

5.6 Conduct a cybersecurity self-assessment or engage third parties to perform a cybersecurity assessment

At OT-CMF Level 2, the self-assessment of an agency's cybersecurity posture becomes a very important indicator of its progress in lowering OT risks. The results will guide the agency in implementing practices and targeting spending at Level 3. The importance of understanding the progress of the organization can't be understated, and the use of a third-party assessor may be a great option if the agency can afford the cost. A third-party assessor will bring skill sets the transit agency may not possess internally, as well experience from assessing other transit agencies. Some assessors will use proprietary tools requiring the tool's continued use to maintain a scoring rationale. Using a third-party assessor should be a calculated and planned process.

For self-assessment, the Cyber Security Evaluation Tool (CSET®) is an option provided by the DHS, but there are other capable tools that can also be used. DHS created the free CSET assessment to assist organizations in protecting critical infrastructure. It was developed under the direction of the DHS ICS-CERT by cybersecurity experts and with assistance from NIST. This tool provides users with a systematic and repeatable approach for assessing the security posture of their cyber-systems and networks. It includes both high-level and detailed questions related to all industrial control and IT systems.

A good self-assessment tool should guide users through a step-by-step process to assess their control system and information technology network security practices against recognized industry standards. The output from the tool should be a prioritized list of recommendations for improving the cybersecurity posture of the organization's enterprise and industrial control cybersecurity systems. The tool should derive its recommendations from a database of cybersecurity standards, guidelines and best practices. Recommendations should be linked to a set of actions that can be applied to enhance cybersecurity controls.

Tools should be designed for easy installation and use on a standalone laptop or workstation. They should also incorporate a variety of available standards from organizations such as NIST, NERC, the Department of Transportation, the Transportation Security Administration, the Department of Defense and others. The goal is to gain visibility, efficiency and the ability to enhance an agency's security posture as a result of performing a self-assessment in a control system environment.

6. OT-CMF Level 3: Operationalized

This level builds upon Level 2 to further enhance and mature the organization's control system cybersecurity program. Attaining Level 3: Operationalize requires organizations to take the steps listed in this section.

6.1 Establish an OT Security Controls Systems Monitoring Program

As the scope and complexity of digital technology at transit agencies has increased, so has the recognition that OT is a valuable target. State actors, organized crime, terrorists and lone wolves are actively attempting to manipulate vulnerabilities in OT systems. Many of the system vulnerabilities are known to a wide variety of people once they are discovered. The issue is that, once identified, these vulnerabilities are not always patched or mitigated immediately by the transit agency for various reasons. Having a view of the systems and the indicators that a threat is exercising the vulnerability provides an opportunity to intercede or manage the incident at an early stage.

Establishing an OT Security Controls Systems Monitoring Program is a significant step in protecting the OT network of systems in the transit environment. It is essential that even systems that are secure by design and have been pen-tested be monitored. Building a program means more than just looking across the OT network. It will also mean that there is oversight, periodic testing, evaluation against goals and adequate funding. When an alert is received in the SIEM/OT threat detection system (IDS), it should include the full context asset description (e.g., location, owner of assets), and there should be operational instructions in place on how to respond to the alert. The response should be in accordance with the severity and potential impact on safety.

Having an OT IDS helps to provide added security and a safety net once the program is launched. The technology and monitoring schemes for OT may vary widely from those employed with enterprise networks. OT systems have a different temperament and require different handling by OT security professionals who understand how traditional approaches like scanning can negatively affect the timing of an OT system.

All agencies are encouraged to deploy technology to improve visibility on OT systems and share those outputs with partners. Each agency must assess and select the technology or provider that is best for it. The

decision to monitor the OT is not an option, and its deep association with detecting, identifying and responding to incidents makes it a critical component to OT security programming.

Collecting logs is very important; however, understanding what the correlation of data is saying is more important. By sharing information and incidents, transit agencies will enhance intelligence of incidents identified in their own networks based on anecdotes and analysis of trusted partners at other transit agencies.

OT cybersecurity requires trained people, processes, and technologies to be utilized in a layered defense strategy to be effective. Security information and event management (SIEM, pronounced "sim") is a key enterprise security technology, with the ability to tie systems together for a comprehensive view of IT security. The SIEM can provide an important capability as part of a cybersecurity toolset. At its core, a SIEM system can provide a central repository for all security events generated in an enterprise. Modern SIEM solutions will include some AI capabilities to provide alert automation and automated behavioral analytics. The analytical components provide functions to review combinations of events to identify suspicious activity. SIEM tools that log everything see very little. In cases where a SIEM tool is used in the OT, it's important to encourage the vendors of the safety/operational equipment to feed it with information to enrich it. Sometimes it doesn't happen out of the box. The agency must have a relationship with its OT vendors.

6.2 Establish a continuous improvement program from the metrics as defined in Level 2, Section 5.2.6

Over time, policies and procedures will need to be improved based on changes in laws, regulations, agency objectives, research and threat intelligence about how cybercriminals exploit weakness in networks. Being agile and continuously seeking to improve approaches to securing OT systems will create a culture of improvement that keeps up with an ever-changing technology environment across transit agencies.

Modernization and approaches to deliver more efficiency while reducing costs leads transit agencies to introduce new technologies. Technology platforms like cloud computing and 5G are driving growth and expanding risks across transit agencies. This is just one reason why risk management must be a living and breathing part of security management. Important to protecting the agency, the policies and procedures that support risk reduction must keep up with the changing environment to ensure that anomalies and issues affecting the agency's security goals and risk objectives are managed appropriately.

As transit agencies grow and add new technology schemes to meet the mission, new risks inevitably will emerge. New technology applications will increase vulnerability, and changes to longtime approaches will need to be augmented when technology architecture and service delivery decisions, like moving platforms off-premise to the cloud, are made to support growth. Not adjusting policies and procedures to account for these changes can create new opportunities for hackers. Hackers exploit weaknesses in technologies but also the seams that are created by disjointed security application. Therefore, changes in policies and procedures should be managed through the Cybersecurity Governance Committee. Security must be orchestrated, and when changes are required in one area of the organization, it is critical to understand what other stakeholders may be affected by the change or what faults the change in policy or procedure might create.

The value of creating risk objectives and goals early in the development of the OT-CMF program can't be overstated. Understanding the goals of the agency for protecting OT assets and the critical services they support early on will make it easier to adjust policies and procedures when the baseline risks and security considerations change. When an agency recognizes, analyzes and categorizes a risk, it determines the appropriate disposition of the risk (common dispositions include avoid, accept, monitor, transfer and mitigate) and identifies response activities. Any determinations that lead to a specific procedure, specific risk disposition assignment or strategies for certain categories of risk may now be so different that the policy or

procedure creates a vulnerability. Identifying the gaps can help the program to stay ahead of hackers who are continuously evolving their approach to network exploitation.

6.2.1 Review and update the recommended controls to align with the agency's security goals and objectives

Every agency will address OT security differently within the context of using available best practices. These approaches will change at each stage of growth and maturity. As an example, some agencies will hire external resources while others will build in-house capabilities.

While implementing OT-CMF recommended controls, it is important to understand that the controls an agency ultimately selects should be those most closely aligned with its goals and objectives. To go a step further, the alignment should also be in step with the agency's risk tolerance and risk objectives. Controls are a capability. They should not be implemented to satisfy a compliance requirement but rather be implemented because they bring value to the security objectives.

6.3 Identify gaps in policies, procedures and current practices across the organization, and develop remediation strategies to ensure compliance

The adversary works 24/7 to undermine agency security and to exercise vulnerabilities (accidentally triggering or intentionally exploiting). In a changing transit environment, the entire team at the agency must continuously identify gaps in policies, procedures and current practices. This is the only way to meet the challenge of securing people assets, information, technology and facilities.

The security program must breathe and allow structured change. NIST explains in NIST Special Publication 800-53 Rev. 5 that even the security controls are meant to be flexible and adjustable. Security assessment never ends, and the more data points available to shape the security approach, the better the security outcomes. Flexibility is achieved through iteration and refinement actions combined with the original assignment and selection operations:

- **Iteration** allows agencies to use a control multiple times with different assignment and selection values, perhaps being applied in different situations or when implementing multiple policies. For example, an agency may have multiple systems implementing a control but with different parameters established to address different risks for each system and environment of operation.
- **Refinement** is the process of providing additional implementation detail to a control. Refinement can also be used to narrow the scope of a control in conjunction with iteration to cover all applicable scopes (e.g., applying different authentication mechanisms to different system interfaces) to allow agencies to satisfy a broad base of security and privacy requirements, mission and business processes, and system levels of implementation.

Each time a control is changed or adjusted, the policies and procedures should get a quick review. The agency should be keenly aware that gaps and omissions may create a threat vector that undermines the security strategy. The schedule for refinement and analysis should be defined by the Cybersecurity Governance Committee, as it also will manage security accountability at the agency.

6.4 Enhance policies and supporting operating procedures by developing, documenting, approving and publishing changes organization-wide

Policies and their supporting operating procedures are a key to providing direction for the entire agency. Each operating unit will develop operating procedures outlined in the policy to fit its needs and ensure that all procedures follow policy. Developing security policies, procedures, training and educational material that

applies specifically to the OT requires living and flexible policies—meaning that they can be adjusted to meet security requirements of the agency that are aligned with goals and objectives.

6.4.1 Managing changes in operational procedures

The following activities are important to managing required changes in operating procedures brought about by regulatory and specific threat mitigation needs. Most of these activities will often not change the policies, just open them for adjustment and enhancement:

- The National Terrorism Advisory System threat level, deploying increasingly heightened security postures as the threat level increases.
- New information about the life cycle of the OT from architecture design to procurement to installation to maintenance to decommissioning.
- Faults in the network topology for the OT security layers, where the most critical communications are not occurring in the most secure and reliable layer.
- Identification that there is not a logical separation between the corporate and OT networks (e.g., stateful inspection firewalls between the networks, unidirectional gateways).
- Continuous efforts to employing a DMZ network architecture (i.e., prevent direct traffic between the corporate and OT networks) that requires adjustments to protect networks.
- Ensuring that critical components are redundant and are on redundant networks.
- Improvements to critical systems for graceful degradation (fault tolerant) to prevent catastrophic cascading events.
- Results from the testing of critical networks to ensure that vulnerabilities will not impact OT operation.
- Identified physical access to the OT network and devices creating a threat vector for the network.
- Changing OT user privileges required to perform each person's job (i.e., establishing role-based access control and configuring each role based on the principle of least privilege).
- Identified requirements for mitigation after testing all patches under field conditions on a test system before installation on the OT.
- Tracking and monitoring audit trails on critical areas of the OT that identify an issue in the current approach to protecting systems.

6.4.2 Utilizing the OT Cybersecurity Governance Committee

The OT Cybersecurity Governance Committee will minimize the risk of unintentionally undermining the security of the OT network. The OT Cybersecurity Governance Committee should play a role in the approval of changes to the subject procedures to avoid impacts from one change in the operational procedures on the other procedures in a different business unit. The goal is to always ensure alignment of procedures and avoid conflicts in the many policies and operating procedures across the agency.

Important to understand is that controls may be affected by changes in the operating procedures. Control can often apply across multiple processes, systems and/or assets in multiple operating units throughout the enterprise. The OT Cybersecurity Governance Committee can help to provide agency-wide control of all operational change activity.

6.4.3 Critical facilities and operations policies

When thinking of critical facilities and operations policies, one's mind might quickly go to physical security. However, in today's technology mix, cyber–physical systems serve critical functions in managing facilities. A digital action can cause a physical reaction. A cyberattack affecting an OT system may inadvertently impact a safety system. Therefore, there must be oversight of the cyber and the physical to ensure that policies and procedures align. When changes are made to these documents, all stakeholders need immediate awareness.

6.4.4 Procurement and acquisition guidelines

Procurement and acquisition guidelines should be embedded into all operating procedures. The agency's safeguard for utilizing third-party service providers or procuring assets must be known to purchasing cybersecurity practitioners and business unit leaders. Addressing security throughout the life cycle, from architecture to procurement to installation to maintenance to decommissioning, will ensure that the connection between the procedures and the policies is made. It is critical that the policies supported by the operating procedures outline these procurement controls and specifically speak to this linkage.

6.4.5 Operating procedures supporting the established policies

A great example is plans for response and recovery. The various plans must be laid side by side and analyzed to ensure that they do not conflict or count on the same resources during a crisis. Many transit agencies have facilities that are remote or spread across a large geographical area. Assessment of risk tolerance affecting policies and procedures should be carefully reviewed for relevance at each facility. All stakeholders (at the facilities and depending on the facilities) should be trained accordingly to inform them of agency expectations. When plans, policies or procedures change, all stakeholders need to be appropriately informed.

6.5 Define status reporting processes—i.e., to senior management, relevant system owners and stakeholders—of any identified issues

The status reporting process is a way to maintain management control in an agency that has a lot of moving parts. If the agency is starting an OT cybersecurity program, it is safe to assume that there is an enterprise security program. There must be a set of established processes that allow leadership to make appropriate decisions and business unit owners to act, or react, accordingly. Delivering the most accurate and timely OT security information to leaders and stakeholders without processes for data collection, analysis, management and communications will make the reporting spotty, which can lead to security failures.

To best achieve the goal of delivering vulnerability status (an important form of intelligence), status of security activities (like vulnerability remediation) and general situational awareness, there must be a set of processes that the agency aligns to and can measure against. Effective situational awareness depends on the timely collection of sufficiently accurate and inclusive risk-relevant data about the critical service (such as the condition of its supporting assets, the discovery of vulnerabilities to which it would be susceptible, the performance of its high-value physical and cybersecurity processes, and the events detected by its physical and cybersecurity safeguards); the fusing of data from multiple internal and external sources; and the analysis of data, which often includes modeling and simulation.

6.5.1 Value of status reporting

When it is done well, status reporting creates situational awareness to improve all stakeholders' understanding of the past, current and projected future state of a critical service supported by OT assets. Even done poorly there is a value to attempting to inform stakeholders. The collection of data, when effectively communicated to relevant stakeholders, supports automated or human decision-making concerning the appropriate actions for preventing the disruption of a critical service or restoring the service to proper function.

Each status reporting activity must be aligned with agency-accepted processes that eventually funnel relevant data to the right person at the right time. An example of important data is the monitoring of security controls. If the applied controls are failing, it should not be new information to leadership after a major event has occurred. Primary stakeholders should have had the knowledge of issues and/or anomalies prior to a cybersecurity event, allowing them to decide if the issue is a priority to protect critical systems.

Information that makes the organization more resilient is only as good as the information reaching a stakeholder who is positioned to act. The status reporting processes should be inclusive of all stakeholders,

both internal and external to the agency. The information flow in the process should include sources that have been identified prior to developing the status reporting process.

Hopefully, the status reporting procedure will provide the information flow that informs a common operating picture (COP). The status reporting processes should create efficiency in reporting and pathways to highlight critical issues, moving them to leadership faster or ahead of the standard periodic reviews. The COP will provide a view of all activity and the ability for senior management to home in on conditions outside the OT security objectives. Status reporting procedures must not inhibit information flow but encourage the inclusion and curation of information that enhances the COP. The COP can also be used to ascertain whether the status reporting process should be improved.

6.6 Evaluate operating procedures, identify efficiencies and implement for each OT-CMF domain

Once the OT cybersecurity program is operationalized, it is important to continuously evaluate the approach an agency is taking in protecting critical systems. The evaluation of operating procedures requires agencies to review data and insights about the operational environment. Data collection and the ability to identify efficiencies and implement change where that change will enhance security outcomes is a goal at the Operationalize level.

The evaluation process is not just looking for areas that require improvement. Agencies should also seek to understand where processes have created efficiencies that can be transferred to other processes and procedures. The cybersecurity audit of the operating procedures can provide management with an assessment of the agency's cybersecurity policies and procedures, as well as the operating effectiveness. The review of procedures can identify internal control and regulatory deficiencies that might put the agency at risk.

A plan for the evaluation of procedures should describe a test-and-evaluation strategy for OT cybersecurity that uses relevant data from all sources and includes testing production representative systems in an operationally representative environment. Data sources may include, but are not limited to, information security assessments, inspections, component and subsystem level tests, and system-of-system tests. The plan should provide details on the cybersecurity test and evaluation strategy—especially if being performed in an operational environment.

The purpose of testing cybersecurity procedures by doing operational testing is to assess the ability of the approach to enable operators to execute critical missions and tasks in the expected operational environment. Testing of cybersecurity should include the representative users and an operationally representative environment that may include hardware; software (including embedded software and firmware); operators; maintainers; operational cyber/network defense; end users; network and system administrators; help desk; training; support documentation; tactics, techniques and procedures; cyberthreats; and other systems that exchange information with the system under test. Some OT environments won't allow this type of testing. In those cases, a walkthrough of the procedure should still be undertaken to evaluate the requirements.

Part of auditing is ensuring that organizations have implemented controls. This means that preventive tools such as firewalls and antivirus software have been put in place. It also means that awareness efforts have been made, and that user education about password construction and backups has been provided. Regular updates—to both preventive tools and awareness efforts—are a necessity. That's why regular audits are so important: Organizations must ensure that these processes are well-designed, executed properly and as up to date as possible.

Cybersecurity audits should be performed no less than annually based on business needs. They should include planned activities with specific start and end dates, including exact expectations and clear communications.

Threats, both internal and external, have the potential to impact confidentiality, integrity and availability if controls are not in place. And the definition of "threat" is broad, encompassing a variety of elements that can impact an enterprise. New laws and regulations or growth in data may pose a threat to the organization. Human threats can include everything from carelessness to espionage. There is an array of technical threats including, but in no way limited to, malicious code, unauthorized access, malware or hardware/software failures.

Adversaries are not limited to exploiting vulnerabilities within the set of frameworks and controls that agencies have established to protect their networks. The evaluation of electronic and physical methods of accessing, using, protecting, maintaining and disposing of OT assets is a continuous process.

6.7 Implement a role-based, organization-wide cybersecurity training and threat awareness program

A top-down approach is often helpful in ensuring that the training and awareness program meets the resilience objectives of the organization. Obtaining support from management is essential to ensuring that the training and awareness plan is effectively implemented. The level of management support required depends on the scope of the training and awareness program being implemented. Senior-executive-level support is necessary for a training and awareness plan that addresses the entire organization.

OT information security training can also be considered an OT workforce development and improvement program. Each organization needs to assess its requirements to determine what the mix of training should be. Agencies should define the knowledge and skill levels needed to perform OT security and system management duties and tasks. The role-based training programs for individuals who are assigned OT system management roles and responsibilities will be very focused and may require external training support. The agency will need to develop standards for measuring and building individual qualifications for both employees and applicants for information security–related positions.

A training and awareness program should be developed to reflect priorities at the enterprise and operating-unit levels, as well as for specific critical services. The following steps illustrate an approach for establishing objectives for a training and awareness program:

1. Identify management directives and organizational priorities. Organizational priorities can be articulated in many forms and help identify the strategic objectives. Strategic objectives are derived from strategic planning activities, which usually forecast two to five years out.
2. Define and document training and awareness program objectives. Training and awareness program objectives are derived from the management directives and organizational priorities identified above.
3. Prioritize training and awareness program objectives. Training and awareness program objectives should be prioritized based on their potential to affect operational resilience.

The following steps illustrate an approach for integrating training and awareness objectives specific to cybersecurity resilience in an existing training and awareness program:

1. Review the existing activities before implementing new training and awareness program activities. This will ensure that new training and awareness activities are not redundant.
2. Review existing training and awareness program activities to determine if they are still effective. This review is often completed as a byproduct of auditing or feedback and measurement activities. A training and awareness program activities assessment should provide sufficient evidence to determine the effectiveness of the implemented training and awareness program activities.
3. Establish new training and awareness program activities to fill the gaps between existing activities and needed ones.

4. Confirm that existing and updated training and awareness program activities are still relevant and assign responsibility for implementation of new activities. Responsibility for ensuring that training and awareness program activities are implemented typically rests with the operating-unit managers.

6.8 Define classification and risk calculation standards to assess risk and qualify/quantify the impact

Cybersecurity risk management is an important factor to ensure the safe and reliable delivery of the goods and services provided and supported by OT. The first steps in information security strategic planning in any form of business are risk management and risk evaluation. This is necessarily broad, including business processes, stakeholders and physical infrastructure, as well as the information system. The security risk evaluation needs to assess the asset value to predict the impact and consequence of any damages. To do this, the agency needs a consistent way of evaluating and classifying assets and systems related to the OT program.

6.8.1 Risk modeling

Risk models differ in the degree of detail and complexity with which threat events are identified. When threat events are identified with great specificity, threat scenarios can be modeled, developed and analyzed. Threat events for cyber or physical attacks are characterized by the tactics, techniques and procedures employed by adversaries. Understanding adversary-based threat events gives organizations insights into the capabilities associated with certain threat sources. In addition, having greater knowledge about who is carrying out the attacks gives organizations a better understanding of motivations of the adversaries.

Identification, valuation and categorization of information systems assets are critical tasks when developing and deploy the required security control for the specified OT assets. Organizations or individuals able to implement security for assets by using this model must first identify and categorize the organization's OT assets that need to be protected in the security process.

Quantitative measurement of risk impact is implemented based on the following formula:

$$Risk\ Impact = Potential\ Risk \times Probability\ of\ Occurrence$$

6.8.1.1 Potential risk

Potential risk could be any type of risk that is conceivable for an agency, or any risk associated with an action that is possible in certain circumstances. This risk also refers to a threat or damage that may occur on operations of the agency. Risk potential should be estimated without a detailed consideration of the individual risk, at as little expense as possible. Potential risk is a product of total asset value, severity of vulnerability and severity of threat:

$$Potential\ Risk = Total\ Asset\ Value \times Severity\ of\ Vulnerability \times Severity\ of\ Threat$$

6.8.1.2 Probability of occurrence

Probability of occurrence is an estimate of how often a hazardous event occurs. The likelihood can be expressed in terms of the frequency of occurrence. A review of historic events assists with this determination.

6.8.2 Integrating modeling with Risk Management Framework

Risk management allows organizations to use simulation to measure risks. By understanding the potential likely outcome, an organization can make better decisions considering those risks. Of course, this form of business intelligence can guide transit agencies in selecting steps most appropriate to reduce identified risks. In the first step of the RMF "Categorize" risk, modeling can be used to understand the potential consequences as well as determine the prioritization of critical systems and services. The second step, "Select" security

controls, requires an organization to develop the appropriate baseline using categorization output from the Categorize step. Baselines will be determined by information and system categorization, organizational risk assessment and the stated risk tolerance, and system level risk assessment. Each organization will learn about its specific requirement from agency goals and objectives compared with its available technology, processes, and personnel. See **Figure 3**.

FIGURE 3
Risk Management Framework

The NIST Special Publication 800-37, Risk Management Framework for Information Systems and Organizations, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf provides insights that will guide a transit agency in plans to manage risks through the risk management process. The agency should develop a holistic and comprehensive risk management process and integrate the RMF into the system development life cycle (SDLC) providing processes (tasks) for each of the seven steps in the RMF at the system level. Successfully navigating these best practices begins with identifying, through modeling and exercise, critical systems/services and the associated dependencies.

6.9 Implement Tier 3 recommended OT-CMF controls identified in Level 2, Section 5.5

Each agency will select security controls that are best suited for its environment and that align with its goals. Please consult the OT-CMF controls guidance to select Tier 3 OT-CMF controls (Appendix B).

6.10 Perform a third-party annual audit of the OT cybersecurity program

A third-party annual audit of the OT cybersecurity program takes a holistic look at people, processes and technology. Cybersecurity audit programs are an absolute necessity and a great way of documenting the comprehensive security efforts, as well as processes for identifying vulnerabilities to close security gaps.

A third-party assessment should be conducted by a qualified OT assessor, who will do the following:

- Provide an objective assessment.
- Provide with a high level of assurance that the information the supplier provides is accurate.
- Reduce the amount of review an organization needs to conduct.
- Provide evidence for compliance.

6.10.1 Third-party assessors

Third-party assessment teams who do not represent any hardware or software manufacturers take an unbiased approach to an agency's system. While internal teams may have critical knowledge of a control system and may even have designed it, third-party assessors can see the high-level view of the control system, as well as the details of it. They will see gaps in a system that internal teams can miss because of their familiarity.

Third-party assessors are doubly important when it comes to OT and ICS, because all control system manufacturers have their own products and solutions for implementation. Agencies need a perspective from experts who are not beholden to any entity. An unbiased third-party assessment team, especially one with a deep understanding of OT systems, can connect manufacturer solutions with industry best practices for solutions that fit an agency's requirements.

A third-party assessment team with an OT/ICS background can connect manufacturer products and solutions with industry best practices and methodologies that meet an agency's requirements. It will fill in the OT knowledge gaps that an internal IT team may lack. For example, assessors with OT backgrounds can provide insight on which security control hardware a system uses that meets global standards. This is especially critical if a control system uses hardware and software from many different manufacturers.

It is difficult to find OT cybersecurity experts with the necessary background to assess critical systems. The cybersecurity industry is expanding and growing at an astounding rate, and the demand for qualified and experienced professionals is fierce. Even when they can't find qualified professionals to hire, many companies are still hesitant to hire outside help. This is not an option for assessments at Level 3 of the OT-CMF. By implementing a comprehensive information security program that includes third-party assessment, transit agencies are exercising the required due diligence.

7. OT-CMF Level 4: Managed

This level builds upon Level 3 to further enhance an organization's cybersecurity program with standardization and optimization to achieve a higher maturity level. Attaining Level 4: Managed requires organizations to take the steps listed in this section.

7.1 Appoint a cybersecurity professional to the board of directors to oversee the cybersecurity initiatives across the organization

The voice of cybersecurity has not quite made its presence on boards of directors like it has for financial and operational risk. There are more agencies recognizing the need for a continuous input of information as more agencies are dealing with cybersecurity exploitation, costs and decisions that are at the board of director level. The digital infrastructure has become a critical function for many organizations.

The inclusion of OT KPIs in a board meeting provides visibility into an agency's network and operational infrastructure. This allows a holistic view of performance and risk, as well as the risk-versus-reward questions. Risks like ransomware should not be a new subject to the board of directors at the point when the agency becomes a victim. In the new digitized environment, cybersecurity should be on the agenda for a Level 4 agency at each meeting, if just for three to five minutes and explained in business risk and mitigation

strategies terms the board of directors can understand. This ensures that all parties are aligned and that agency policies adequately cover identified risk.

There is full recognition that a cybersecurity professional may not be officially appointed to the board of directors; however, IT and OT have become critical to an ever-digitizing agency environment. If no cybersecurity professional is appointed as a board member, then an existing board member or appointment should have a very strong cybersecurity acumen. This should be an individual who consults regularly with the chief information security officer or other agency cybersecurity executive to minimize the board's blind spots.

The board of directors should have a clear understanding of the following:

- **Statement of applicable laws, regulations and obligations:** The board needs to understand what legal, regulatory, and contractual obligations apply to the organization with respect to cybersecurity.
- **Inventory of data:** The board of directors needs to be aware (at a high level) of the volume and types of sensitive data that the organization stores. It should receive a high-level inventory of the sensitive data and accounting of critical systems.
- **Risk assessment report:** Organizations should have a cybersecurity risk assessment report produced by a third party, with a one-page summary suitable for an annual presentation to the board.
- **Cybersecurity controls assessment:** This controls assessment should be based on a widely accepted framework, such as the OT-CMF, NIST Cybersecurity Framework or similar. This type of assessment typically evaluates the current cybersecurity program, compares it with the organization's cybersecurity goals, and helps define a prioritized plan to increase cybersecurity maturity over time.
- **Technical test results:** Each organization should have annual security assessments that vary depending on the organization's needs.
- **Cybersecurity insurance policy and summary of coverage:** Insurance coverage should be selected based on the anticipated residual risk to ensure that appropriate risks are transferred. Coverage should be aligned with the board's stated risk appetite.
- **Third-party service provider oversight:** This report should summarize the list of third-party providers with access to sensitive data or IT resources, and the results of the vetting process (a simple letter grade or other indicator of cybersecurity risk rating would be sufficient, along with the date of most recent review).

7.2 Establish a formal, self-contained cyber-intelligence program with independent analysis capability

Creating and developing a cyber-intelligence program in an agency requires the support of leadership and agency processes that allow external information flow into the agency. Just as important are the processes for receiving situational awareness information and the required partnerships to see the complete picture. These trusted partnerships will be with government, the private sector and academic partners. Creating and managing the program will require in-the-moment decision-making as information is received and observations about potential exploitation are made. Therefore, the executive leadership must be fully onboard. They must ensure proper policy, as well as the funding that sustains the program, making sure the agency can staff properly, have the freedom to bidirectionally share cyberthreat information, and respond appropriately to cybersecurity incidents.

Visibility of systems and the training for stakeholders that supports a recognition of cyberthreats is heavily dependent on policies and procedures that extend across the agency. At Level 4, many of these policies should be present. However, there are several specific actions and considerations necessary to move external services under internal control and daily management.

The agency must implement the processes and tools required to improve their visibility and understanding of the adversary, their motivations, and their capabilities, as well as the attack surface. Business unit owners must be apprised of the flow of information about critical systems and assets to the in-house team.

The agency must have the capability, through the acquisition of talent and tools, to receive threat intelligence feeds, analyze information, correlate data, and deliver in-house detection and attack surface management services to aggregate intelligence from various providers.

The agency should use an iterative process to build capacity and ensure capability. There are six key principles: planning and direction, collection, processing and application, analysis, dissemination and integration, and evaluation and feedback. The capabilities and funding to support these principles should be in place at program initiation:

- **Planning and direction:** This is the foundational step in building a threat intelligence program. It helps clarify the need, determine the objectives and set the goal for the program.
- **Collection:** In this phase, the cybersecurity team prepares a plan for collecting and storing information from identified sources.
- **Processing and application:** Once the data is ingested and stored in the database structures, it needs to be processed in a way that can be readily consumed and exploited to its maximum potential.
- **Analysis:** Once intelligence starts flowing in and correlation rules and alerts are generated, analysts take over the task of fusing the data points within the threat intelligence stream.
- **Dissemination and integration:** The cyberthreat intelligence team should identify the stakeholders and recipients of threat information and accordingly set up communication/integration channels and processes within the organization and externally.
- **Evaluation and feedback:** To ensure that the threat intelligence program remains relevant and continues to add value to the organization, continuous evaluation and feedback must be instituted throughout the program life cycle.

Cybersecurity at every organization should be evaluated to understand the cost versus benefit of expenditures. Cyberthreat intelligence teams have a financial impact on agencies, and the value of the operation should be calculable. All aspects of the program should be definable, measurable and have impactful metrics.

7.3 Standardize and optimize the established policies, standards and procedures to protect, detect, respond and adapt to the changing threat landscape

Standardizing polices across an organization for OT cybersecurity allows an agency to develop well-informed security standards and guidelines. As noted, these standards and guidelines will change at an agency with evolving threats, regulations, new laws and the maturity of the agency's capabilities. At Level 4, the agency will have base policy, standards and procedures in place. However, the deliberate optimization of these standards and procedures will enhance the ability to protect, speed detection, create more effective response and allow the agency to adapt to changing environments.

The ability to adapt policies to an ever-changing threat environment requires an agile and flexible security system. To use an American football analogy, think about the defense. The defensive unit has a base defense that it regularly uses to stop the offensive team. However, the schemes employed for an offensive team that utilizes more running are different from the schemes for teams that utilize more passing plays. In fact, plays can be changed, and even key players substituted to manage the differing challenges on the field.

To achieve this enhanced environment there must be a strong linkage between the board-level executives and the daily activities that identify what policies should be and how they are implemented. The strength KPIs

will provide visibility into the agency's management of cybersecurity-related activities and performance that supports adjustments that optimize the ability to protect, detect, respond and adapt in near–real time. The KPIs of the control system are used to measure the performance of the system and its sub-systems. These KPIs are calculated in the baseline measurement, in which no additional cybersecurity measures are implemented, to form the basis of the performance of the system.

ICS security may include elements of resilient physical design (redundancy and physical adaptability), in addition to information security, to maintain acceptable system availability. Such requirements are determined by a process of careful risk analysis and system engineering. All practices implemented to get to Level 4 will define an agency's success in standardizing and enhancing policies, guidelines and procedures. Organizations should develop and maintain an enterprise cybersecurity risk management plan that includes security, legal and procurement priorities and accounts for risks associated with the OT network.

7.4 Enforce role-based organizational control systems cybersecurity training and awareness for all stakeholders and require certifications

As previously discussed, training and awareness is critical to developing a culture of cybersecurity. The value in creating this environment is that internal and external stakeholders will use best practices even when they are not being monitored. Training and awareness both serve a purpose of exposing team members to vulnerabilities, threats, policies and procedures, as well as the consequences of not following procedures and policies.

As the agency grows its cybersecurity capability, the need grows for individuals in specific roles and those who represent business units to receive specific training. The agency should seek to provide team members with training that provides a certification from an accredited organization. Certifications are a mark that the professional has achieved the completion of a relevant OT cybersecurity curriculum.

The following document provides information on a training methodology for the development of training for personnel with cybersecurity responsibilities: NIST Special Publication 800-16 Rev. 1 (2nd Draft Version 2), "A Role-Based Model for Federal Information Technology/Cyber Security Training."

7.5 Secure infrastructure design with network segmentation to ensure limited user and device access

The most effective security approach is to build security into the architecture of the system. This means using best practices for network design and operations. This strategy begins with segmenting networks based on their criticality and access requirements. NIST defines network segmentation as "splitting a network into sub-networks…by creating separate areas on the network which are protected…to reject unnecessary traffic. Network segmentation minimizes the harm of malware and other threats by isolating it to a limited part of the network."

7.5.1 Partitioning control systems

A successful Defense-in-Depth approach requires transit agencies to partition control system components and functions into distinct zones based on specific security requirements. It is further recommended that the types of zones be limited to simplify the application of consistent controls. Each zone will require a unique security focus and strategy.

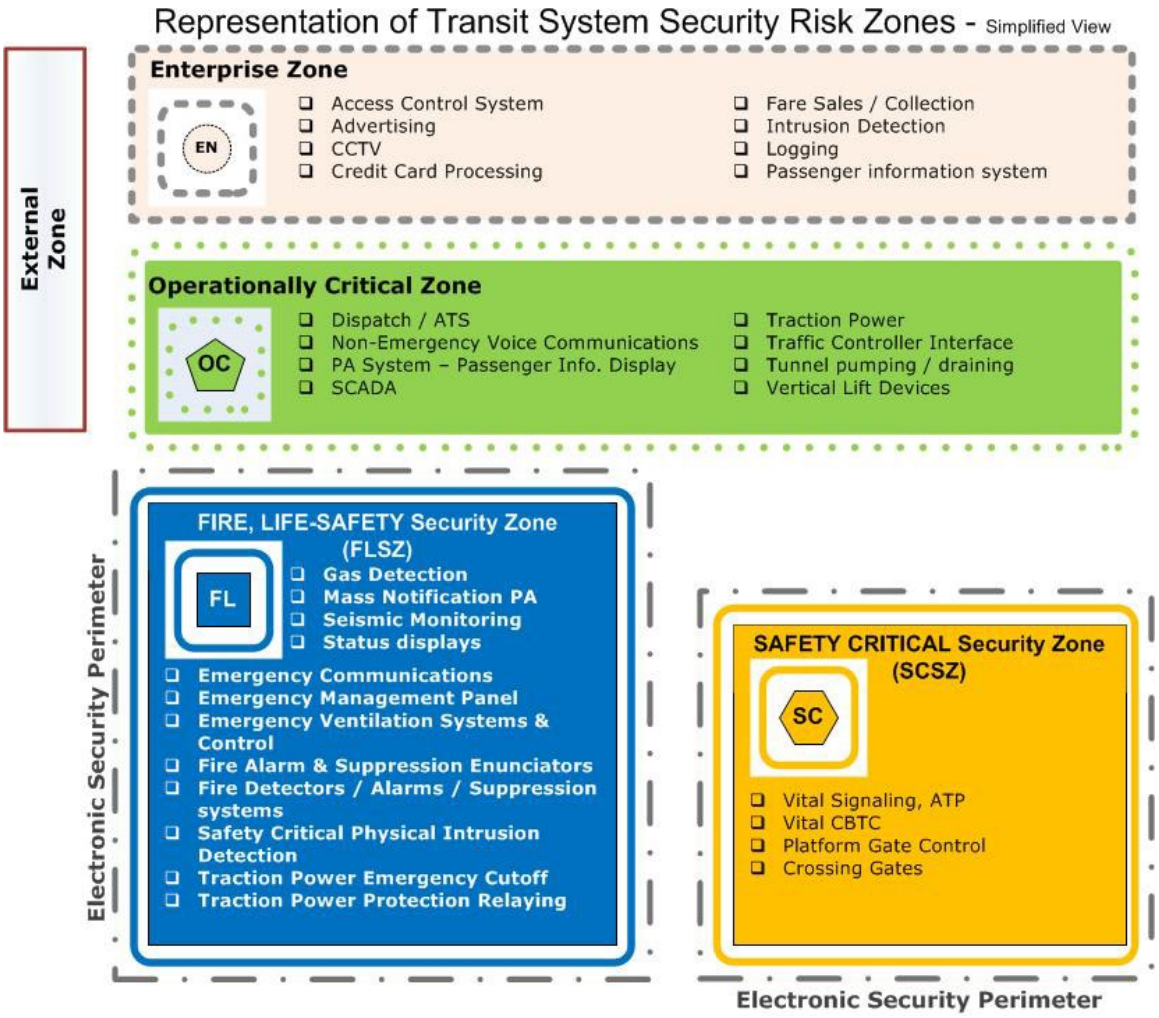
Architectural security zones segment hardware, software and networks into physically distinct areas with well-defined connections between them. Commonly, each architectural zone is managed by a separate business unit and is protected by a dedicated device, perhaps a firewall or other controlled device.

Cybersecurity risk zones (also known as impact zones) segment system functions into distinct impact areas with well-defined data exchanges among them. Cybersecurity risk zones present special planning challenges. They exist within each architectural zone and potentially across them. Different business units may need to establish joint responsibilities in the security management and monitoring of a specific cybersecurity risk zone.

7.5.2 Representation of transit system security risk zones

Figure 4 shows an example system's security zones in the aggregate, and how they relate to the functions needed by a typical transit agency. Note that the SCSZ and the FLSZ should have separate ESPs, and that each of the other zones needs the appropriate level of protection for its zone.

FIGURE 4
Transit System Security Risk Zones



7.5.2.1 Operationally Critical Security Zone

- **Should include:** Traction power, ATS, dispatch
- **Should not include:** Anything from SCSZ, External Zone or Enterprise Zone

7.5.2.2 Fire and Life-Safety Security Zone

- **Should include:** Fire; hazard; monitors for seismic, biologics, poison gas; traction power emergency shutdown systems
- **Should not include:** Anything from SCSZ, External Zone or Enterprise Zone

7.5.2.3 Safety Critical Security Zone

- **Should include:** All "vital" systems for signaling and interlocking, ATP
- **Should not include:** Anything from other zones (External, Enterprise, OCSZ, FLSZ)

7.5.3 2021 Security Directive

Protecting the OT environment is important to network security; however, it is also a requirement for many agencies under the 2021 Security Directive 1582-21-01, "Enhancing Public Transportation and Passenger Railroad." The SD requires that agencies conduct a cybersecurity vulnerability assessment using the form provided by TSA and submit the form to TSA. The vulnerability assessment will include an assessment of current practices and activities to address cybersecurity risks to information and operational technology systems, identify gaps in current cybersecurity measures, and identify remediation measures and a plan for the owner/operator to implement the remediation measures to address any identified vulnerabilities and gaps.

Without network segmentation, some agencies will be challenged to meet the spirit of the SD. Building in security through network segmentation will enhance security and assist agencies in meeting requirements for addressing cybersecurity risks for IT and OT systems. At Level 4, agencies should be able to perform at the level identified above. Activities like identifying vulnerabilities and gaps should have been implemented at Level 3 and be well-honed at Level 4.

7.5.4 Key rules for network segmentation

- The industrial network should be completely segregated from the corporate information system and external networks, especially the internet.
- Industrial process and equipment status information should be sent to the corporate information system via a special gateway. It should be unidirectional, only outward to the corporate enterprise system. The most secure implementation is via a DMZ following the guidelines of NIST 800-82 Rev. 2, "Guide to Industrial Control Systems (ICS)." Security control commands should not be sent from the corporate information system to ICS components or to gateway hosts.
- The Management Information System (MIS) or Supervisory System gathers data from gateways at multiple industrial facilities, which may be geographically distant from one another. The corporate information system segment containing MIS components is separated from the other segments; it may include analyst and manager workstations for processing data.
- Industrial process control, administration and security of the industrial network are performed only by special staff inside the industrial network.

7.6 Implement security orchestration, automation and response (SOAR)

Security orchestration, automation and response (SOAR) platforms are a wise investment and a highly strategic decision for a mature cybersecurity operations environment. Security orchestration is the machine-based coordination of a series of interdependent security actions across a complex infrastructure. SOAR technologies strive to automate some of the repetitive human effort required to maintain a strong security posture. The SOAR platform serves as a central part of a security infrastructure, effectively acting as the operating system for security investments.

Security automation is the machine-based execution of security actions. Security response is the policy-based coordination of human and machine-based activities for event, case and incident workflows. This allows an

agency to play to its strengths. Humans do human work, and the machines are aligned to perform calculations to identify, detect, manage and respond to situations at machine speed.

7.6.1 Role of the analyst

SOAR is one of the best solutions for detecting modern threats. SOAR tools make it easier to get a full 360-degree view of incidents and threats if the systems are properly set up. Based on the NIST CFS, organizations should be able to detect anomalies and events and have continuous monitoring. Through SOAR, all of this is automated. Cases can be analyzed based on an agency's criteria, and the system can close cases that are false positives or put them in a containerized situation until the analyst can do further analysis.

SOAR can communicate, support analysis and mitigate threats. However, in most cases the analyst will still be required to support additional evidence-gathering and investigation to determine the best course of action for the agency. Then, once a threat is analyzed, an analyst can run a playbook against it to automate the future response.

7.6.2 Incident response capabilities

Incident response is a critical component of a cybersecurity program. The business capabilities and functions required to support incident response include:

- **Identification:** Knowledge of assets and where they reside with appropriate controls and protection.
- **Protective capabilities:** Policies, education, access controls, protection procedures.
- **Detection:** Capabilities to detect anomalies and events.
- **Response:** Playbook, regular cybersecurity exercises, coordinated efforts across business units.
- **Recovery:** Remediation and after-action improvement.

In today's cybersecurity climate, agencies should assume that hackers will penetrate the network. The SOAR technology will improve the speed of response and provide analysts with information to support evidence collection and containment activities.

Key parts of the incident response practice are tamper detection and auditability. This capability ensures that appropriate personnel are notified of unauthorized or abnormal activity, allowing for a timelier response. Transit agencies need to identify the systems, devices and processes that are most important or are most easily corrupted. Notification mechanisms must be installed to integrate with the system and provide awareness when it is not operating as intended, when there is unauthorized access, or when observations are out of line with preset system performance levels.

7.7 Integrate security controls monitoring program with enterprise security information and event management (SIEM)

Security controls are an agency's initial approach to managing risks and weaknesses in systems. They can be individually applied to meet a requirement and even be coupled with other controls to close the security gap. At this tier in the OT-CMF, the agency should integrate the security controls program in part with the SIEM. There are two immediate advantages:

1. Every event and the selected control related to the event will be identified.
2. An agency can more immediately adjust controls to better manage unintended or unidentified gaps in controls.

The goal is not to build a highway of information that flows into a SIEM. Rather, the SIEM should detect, collect and correlate, making it easier for the analyst to manage the most important information and alerts.

An OT SIEM can also act as an operating tool, improving uptime from unplanned outages due to anomalous patterns that have no malicious actor, but instead come from defective or problematic system function.

Visibility from a monitoring program is critical to incident detection and response plans, procedures and methods that are necessary for rapidly detecting incidents, minimizing loss and destruction, preserving evidence for later forensic examination, and restoring OT services. The costs associated with obtaining a network view of the OT systems is minimal compared with the cost associated with isolating and mitigating a malware infection or restoring systems that may not be readily available. Conversely, establishing a successful incident response capability includes continually monitoring for anomalies; prioritizing the handling of incidents; and implementing effective methods of collecting, analyzing and reporting data.

Deploying this integrated approach at the enterprise level will help risk managers to better understand hidden risks. Instead of just identifying the issues, the system can be manually or automatically adjusted to get closer to the risk objectives. This approach will unite the performance of IT and OT systems but will have the capability to understand where the systems diverge to minimize the unmanaged influence enterprise IT may have over OT considerations. SIEM tools can be purchased and honed, whereas SOAR always includes third-party integrations and encompasses the next generation of cybersecurity systems.

7.8 Automate mitigation of vulnerabilities with clearly defined service level agreements/operation level agreements (SLAs/OLAs)

Security vulnerabilities represent a flaw or weakness in system security procedures, design, implementation or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy. Vulnerabilities are commonly mitigated with security controls.

To automate mitigation of vulnerabilities requires the agency to employ mechanisms used to schedule, conduct and document maintenance and repairs. The monitoring systems are not necessarily part of, or connected to, the OT. The fragility of some OT systems doesn't allow the use of commercial systems potentially used in IT environments. OT professionals must be careful to systematically test and manage technologies being deployed to deliver controls in an automated fashion.

In situations where the ICS cannot support the specific maintenance requirements of a control, agencies should employ compensating controls in accordance with the general tailoring guidance. Examples of compensating controls are given with each control as appropriate in NIST 800-82 Rev. 2:

- Agencies need to determine whether the use of integrity verification applications would adversely impact the operation of the ICS and employ compensating controls (e.g., manual integrity verifications) that do not affect performance.
- Agencies should ensure that the use of integrity verification applications does not adversely impact the operational performance of the ICS.
- In situations where an agency cannot employ automated tools that provide notification of integrity discrepancies, it should employ nonautomated mechanisms or procedures. Example compensating controls include performing scheduled manual inspections for integrity violations.
- The shutting down and restarting of the ICS may not always be feasible upon the identification of an anomaly; these actions should be scheduled according to ICS operational requirements. In situations where the ICS cannot detect unauthorized security-relevant changes, the agency should employ compensating controls (e.g., manual procedures) in accordance with the general tailoring guidance.

7.9 Establish processes and technologies to report emerging threats to the board of directors

Security programs should be developed in layers. Applying unnecessary assets and technologies is costly and creates security issues. By following the OT-CMF, when an agency reaches Level 4 the agency will have the foundation to provide the data necessary to inform the processes and technologies supporting board of director oversight. Specifically, the organization will have orchestrated security activities, controls, management, evaluation and playbooks for response to all produced datasets of emerging threats at a speed most organizations struggle with today.

Boards of directors are the ultimate risk managers for the agency and must make decisions to lower a variety of risks or decide on an appropriate disposition to avoid, mitigate, transfer or accept risks. A part of that responsibility is to put practices in place allowing the visibility of trends and emerging OT threats that increase risk. The board depends on the policies, practices and professionals within the agency to identify anomalies, trends and potential failures. This supports a capability to get ahead of impactful consequences from predicted and unpredicted events. Therefore, the board must continually push the improvement of indicators and processes that ensure that they are never in the dark.

The optimum position for a board of directors in managing a technology security environment is to receive curated and perfectly designed information sets that allow them to make risk decisions based on all the most impactful information available. As vendors and researchers work toward this state of cybersecurity management, agencies should continue putting the OT-CMF best practices in place that will one day inform this capability.

Key to meeting the challenge of managing the security growth of the agency is identifying what to report, how to report it, when to report and the format. Boards of directors need to have a participant with a strong cybersecurity acumen who has the authority to implement processes that best position the board to make critical decisions. Some critical decisions are made on the spot, like in the instance of ransomware, and others are longer-term decisions. An example is whether it is prudent based on maturity, costs and timing to purchase and deploy a SOAR system. In all situations, the board must be positioned to receive and understand the information most appropriate for performing their duties.

7.10 Engage third parties to perform an annual audit of the operational technology cybersecurity program

As discussed earlier, third-party assessment teams should be independent and not representatives for hardware or software manufacturers, who can take an unbiased approach to an agency's system assessment. While internal teams may have critical knowledge of the agency's control system and may even have designed it, third-party assessors can see the high-level view of a control system as well as the intricate parts of it. They will see gaps in a system that internal teams can miss.

An unbiased third-party assessment team can connect collaborative solutions with industry best practices that inform security advancement (that fit the agency's requirements). Some cybersecurity leaders are now convinced that the current methods of third-party assessment are becoming obsolete and even this approach should be matured. This opinion is based on the rapid growth of digitization and ever-growing threat to digital systems. Specifically, they argue for more robust assessment ecosystems that bring the collaboration of cybersecurity defenders while maintaining trust and confidence in having outsiders working within the agency.

Agencies are looking at joint ventures and alliances that provide both immediate security maturity and the tools to achieve long-term strategic approaches that lower the cost of security. At this level, third-party

collaborations will emerge and accelerate with the speed of digital evolution. The current pace of change will manifest into risk communities and ecosystem that share security mechanisms, such as threat information and tools. This will allow agencies to stay current and embrace disruption more effectively. Transit agencies with mature OT programs will achieve a competitive defense against in the cyber theft market. Suppliers, contractors, joint ventures, service providers, brokers, agents and consultants will be a part of a platform that incentivizes plug-and-play partnership.

As transit organizations form relationships and build partnerships through consortia that are ever-growing, the risks grow also. However, the risks lie not only in the relationships themselves, but also in the contracts that bind the organizations together. Leadership at transit organizations are ultimately responsible for managing them.

Cybersecurity experts with the necessary backgrounds will become more difficult to find as the cybersecurity needs expand for all critical sectors. At this level, assessors will have specialized tools and targeted approach to ascertaining risks specific to the agency. Automation and efficiency will enhance assessment maturity.

8. OT-CMF Level 5: Optimized

This level builds upon Level 4 to fully mature the organization's cybersecurity program. Attaining it requires organizations to have the features listed in this section.

8.1 Security orchestration to monitor, hunt and react to potential zero-day threats and vulnerabilities

To combat today's threats at an advanced level, an agency needs a next-gen SIEM that leverages the architecture and security capabilities that are best suited to detect both known and unknown threats within its environment. The SIEM needs to be a part of the security orchestration to monitor, hunt and react to potential zero-day threats and vulnerabilities. Level 5 agencies possess this capability and the technical prowess to inform the community of the information they obtain while proactively defeating cyber-exploitation.

A zero-day threat is a vulnerability that is actively exploited by attackers while remaining unknown to the vendor or threat intelligence outfits. Once the vendor becomes aware of the security flaw, day zero, it can start to mitigate against exploitation, but not before. The attackers, therefore, have a head start. A Level 5 agency network will identify network anomalies and make a comparison to known signatures and TTPs. If there is no match and the determination is made by the system that the activity matches the behavior of cyber-exploitation, it will take actions to avoid network exfiltration or disruption until an analyst can assess the anomaly.

This may sound like capabilities shared across many of the organizations at a lower level of OT-CMF maturity. The difference is the ability of the system to hunt for threats and the trust in the automated system to act. Threat-hunting is a proactive strategy to search for signs of threat actor activity to prevent attacks before they occur or to minimize damage in the event of a successful attack. Automating threat-hunting can help an agency accelerate network security processes, reduce operating costs and improve its capacity to mitigate advanced cybersecurity threats in time to break the "kill chain."

CISA and the FBI advise that transit agencies can better assess system, user, endpoint and network activity patterns by understanding the IT environment's routine activity and architecture. These insights will be based on establishing a baseline underpinned by a well-honed behavior-based analytics approach. This approach can help an organization to remain alert to deviations from normal activity and detect anomalies. The system can't just collect logs. As an example of other functions, it must be able to help find the needle in the haystack. The return on investment is great with this approach because it will also provide performance indicators for the

systems being monitored. The baseline environment—including the normal internal and external traffic—can help in detecting anomalies. When combined with advanced analytics and artificial intelligence technologies, suspicious traffic patterns can quickly and automatically be explored by the system.

Among other activities, the capability will review and correlate across the following:

- numerous failed file modifications
- increased CPU and disk activity
- the inability to access certain files
- unusual network communications and signaling
- vibrations in the intrusion prevention systems and automated security alerting systems, such as security information event management software, intrusion detection systems, and endpoint detection and response
- usage of deployed honeytokens and alerts signaling the detection of lateral movement

A lot of agencies are employing some aspect of these techniques today. The goal is to get the security measures working in unison without the direct interaction of humans to produce the security effect that identifies zero-days and known cybersecurity exploits to automatically manage the risk they pose.

8.2 Advanced proactive processes with tools and technologies to protect, detect, respond and autonomously adapt to a changing threat landscape

The implementation of advanced proactive processes with tools and technologies to protect, detect, respond, and autonomously adapt to a changing threat landscape requires the proper information feeding the capability and the situational awareness that defines the changing threat landscape. If there is a flow of "garbage in," the system will break down, and the enhanced results will be minimized. Advanced proactive processes tie in traditional robotic process automations brought in through SIEM and SOAR that should be negotiated and applied via AI as they apply ML to passively identify threats, assess risky situations, and propose and actively pursue incident response measures.

A best practice for an IP-based OT network is to have very granular network segmentation and baseline data for all Layer 3 and Layer 4 headers expected on the OT network. Access control lists (ACLs) should be tailored as tightly as possible (based on the predefined Layer 3 and Layer 4 header information) on OT router interfaces for each subnet, so as only to allow known traffic intended for the one or few OT devices in that subnet. Logs of filtered packets should be sent back to the Security Operations Center (SOC) or data aggregation location of choice.

NetFlow version 9 and IP Network Flow Information Export (IPFIX, based on NetFlow) are examples of mechanisms to capture information in packet headers and forward this data to a collector in an SOC. There is now an IPFIX equivalent available on some routers to collect data such as all fields in IPv4 or IPv6 headers, portions of packet payloads, routing information, timestamps, packet counts, etc. A best practice is to put the onboard OT network behind a next-generation router firewall and enable Flexible NetFlow on this router firewall to forward flow data to the SOC. Another best practice is to enable complete packet capture via an application such as Wireshark or tcpdump and the ability to send this data to the SOC.

For OT networks that are not IP-based (e.g., IEC 61375, CAN bus), it is also useful to insert a monitoring device, or data sensor, on the bus to monitor traffic and detect intrusions. These data sensors should be able to decode the protocol and analyze the traffic, as well as recording traffic as a bitstream. Data sensors for non-IP networks should themselves also have a secure IP connection back to the SOC.

A key resource to optimize the system's understanding of the landscape, MITRE ATT&CK® is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. This site includes a matrix of general types of techniques, spanning reconnaissance, resource development, initial access to command and control, exfiltration, and impact. Under each type of technique is a listing of specific techniques, which can be expanded into sub-techniques. Both techniques and sub-techniques include mitigations and detection methods.

A Level 5 optimized cybersecurity program will implement both the mitigations and the detection methods for all the cyberattack techniques listed in the MITRE ATT&CK Matrix. There is also a Navigator version of the MITRE ATT&CK on which one can look up the various techniques used by specific cybersecurity enemies, as well as details of specific attacks. If an enemy or a malicious tool is known to attack critical infrastructure, their known techniques may be listed in MITRE ATT&CK Navigator. A Level 5 best practice is to automatically use such data to search for and discover any known attack, as well as any new variation of known attacks—the latter being zero-day attacks—and respond autonomously.

The security operation center needs to process a vast assortment of incoming data. This includes OT system logs, Flexible NetFlow data, packet captures, industry and government security tips, and the MITRE ATT&CK data. To successfully prepare for a cyberattack and automate as previously discussed, there must be a complete understanding of the organization's network environment. This includes its information, assets (human or otherwise), components, threats to capabilities, and vulnerabilities. Most importantly, the agency must understand the impact of automated actions across the agency. Impact analysis will assist to mitigate potential conflicts, build confidence in the system, and provide a measure should the system have to make automated adjustments.

8.3 Automated and optimized processes to continuously monitor and improve operations technology cybersecurity controls' efficiency and performance

The continuous monitoring activities within an agency are important to understanding the shifting risk conditions and the delta between the risk object's goals and the target. Automation allows the capability and capacity to understand these indicators in near real time. The benefits of automated operations are improved productivity, reliability, availability and performance, as well as reduced operating costs. This makes the security of systems a value proposition because resilience and efficiency are outputs of honing operations.

The goal is to go a step further and achieve this same value from the controls that are in place to protect the agency's network. This means the agency is working toward improved productivity, reliability, availability, performance and operating costs from the security system. This optimization of the controls is key to continuously finding gaps and making improvements to ensure that resources are applied to getting the agency as close to its goal as possible. By working to optimize processes, the agency will gain a sense of control to predict potential issues. Processes will improve to make activities more efficient and ultimately deliver a higher level of performance for the entire OT network.

8.3.1 Role of sensors

The complex interactions of the networks and the sensors that inform them are often overlooked. This is a critical error in managing OT security systems. The OT environment brings together cybersecurity and engineering, backed by organizations that often have different perspectives. This unscripted security interaction can spell security failures for the agency. The interference of sensor function for both intended and unintended disruption has a profound effect on secure engineering networks. More and more, cybersecurity professionals count on sensors to guide the situational awareness of OT networks. The continuous monitoring must account for information being acquired from sensors. Engineering devices (process sensors, actuators,

drives) are important to understanding the condition of the operating environment and can also cause failure, as they have in several major transportation accidents.

8.3.2 Embedded/included software

Transit agencies use equipment and software that is provided by vendors that integrate systems to provide a seamless system. The suppliers of this hardware and software often rely upon code that they did not develop or do not maintain. This makes it very challenging for digital security professionals across transit agencies to ensure the security performance of all systems. Some examples of embedded software include the following:

- an open-source web server
- electronic file-transfer utilities
- remote management utilities
- sensors and automation systems

8.4 Real-time reporting of organizational threats and vulnerabilities to senior management

After reaching Level 5, an agency will have a full-fledged cybersecurity shop with policies and processes that are constantly adjusting to meet the changing threat landscape. Employees will receive role-based training, and automation will hone all security performance to deliver optimum output. And with all this real-time reporting of organizational threats and vulnerabilities to senior management, it will still be a challenge to manage.

Even some of the best-resourced companies that adhere to rigorous governance standards with robustly funded cybersecurity programs will continue to fall victim to cybersecurity incidents and their far-reaching consequences. Hackers are determined, and computing power makes them even more powerful. Too much information is not always good for management. For example, decisions by senior officials to authorize automated risk-based decisions related to the operation of systems, use of common controls, accepted practices, and the risk to organizational operations and assets will come after a well-curated picture is established. Real-time reporting will put the leadership on the front lines, and they will either tune out or dial in too deeply. OT cybersecurity professionals must ensure that the implementation of these systems is adequately managed, and that information is channeled to filters that structures data being delivered to leadership based on prioritization and severity. Transit organizations should utilize a cyber severity scoring system to achieve this ranking. This will help an organization dedicate resources appropriately and help to prioritize what is eventually highlighted in board-level briefings. One such scoring tool is the CISA National Cyber Incident Scoring System: https://www.cisa.gov/uscert/CISA-National-Cyber-Incident-Scoring-System.

The development of systems providing real-time threats and vulnerabilities to senior management should deliver information that is analyzed against organizational goals, risk objectives and distinct KRIs. The information should be self-adjusting and affixed to a GUI that amplifies the change or potential impact.

8.5 An annual third-party audit of the OT continuous monitoring and automated response system

At Level 5, the third-party audit should be a part of the OT continuous monitoring and automated response system. The audit should be built into the system and work in tandem with the continuous monitoring process. The human assessor will be assessing the performance of the system and flaws that may be exacerbated by the magnification of application vulnerabilities or “bad data” inputs.

Risk assessment is just a step in the risk management procedure. It is the determination of quantitative or qualitative value of risk related to a concrete situation and a recognized threat. However, situational change

can itself increase the likelihood or impact of an attack if not calculated in risk management exercises. At Level 5, the system will be performing the risk assessment functions in real time. This means that a third-party assessment will require someone to verify that the automation in the OT system is indeed managing risk through automated controls application, continuously honing the system, and delivering a performance evaluation shortly before it makes authorized adjustments to itself.

At Level 5, the risk is that flaws in the automated systems will not be identified and will grow in time. The susceptibility to attacks lies beyond merely the technical realm, yet many organizations will continue to invest heavily in equipment acquisition. The future of OT cybersecurity will indeed mean investing in these tools, but most important will be the ability of assessment professionals to manage risk from the system by identifying and recommending adjustments, ensuring that agencies are receiving a return on investment. An orchestrated and automated cybersecurity system will solve many problems. However, without the proper management, it will create others.

The assessor should be able to accurately identify and quantify cybersecurity risks across the wide array of internal and external variables, in addition to estimating financial loss potential and cybersecurity insurance coverage gaps. By framing cybersecurity in business terms and predicting growth of flaws in the automated systems, the human assessor will convey requirements understood across technical and nontechnical leadership. They will be the key to providing a defensible framework for risk management decision-making so executives can right-size investments into cybersecurity budgets and future initiatives.

There should be no financial cost to develop or gain access to resources and documents that support OT-CMF implementation. Resource requirements are limited to staff time and the cost of service and technologies to meet an agency’s requirements.

References

Cybersecurity and Infrastructure Security Agency, "Best Practices for Industrial Control Systems," June 2021. https://www.cisa.gov/sites/default/files/publications/Cybersecurity_Best_Practices_for_Industrial_Control_Systems.pdf

ISA Global Security Alliance, "Security Lifecycles in the ISA/IEC 62443 Series: Security of Industrial Automation and Control Systems," October 2020. https://www.isasecure.org/en-US/Documents/Articles-and-Technical-Papers/ISAGCA-Security-Lifecycles-whitepaper

MITRE Corporation, 2016, "Finding Cyber Threats with ATT&CK™-Based Analytics," 2017. https://www.mitre.org/publications/technical-papers/finding-cyber-threats-with-attck-based-analytics

National Institute of Standards and Technology (NIST), "Approaches for Federal Agencies to Use the Cybersecurity Framework," NISTIR 8170, March 2020. https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8170-upd.pdf

National Institute of Standards and Technology (NIST), "Assessing Security and Privacy Controls in Information Systems and Organizations," NIST Special Publication 800-53A Rev. 5, January 2020. https://doi.org/10.6028/NIST.SP.800-53Ar5

National Institute of Standards and Technology (NIST), "Automation Support for Security Control Assessments," NISTIR 8011, June 2017. https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8011-1.pdf

National Institute of Standards and Technology (NIST), "Cybersecurity Framework Version 1.1 Manufacturing Profile," NISTIR 8183, 2020. https://doi.org/10.6028/NIST.IR.8183r1

National Institute of Standards and Technology (NIST), "Developing Cyber-Resilient Systems: A Systems Security Engineering Approach Publication," December 2021. https://csrc.nist.gov/publications/detail/sp/800-160/vol-2-rev-1/final

National Institute of Standards and Technology (NIST), 2017. "Framework for Improving Critical Infrastructure Cybersecurity," Draft Version 1.1, January 2017. https://www.nist.gov/document/2017-04-11-ernstyoungpdf

National Institute of Standards and Technology (NIST), "Guide for Conducting Risk Assessments," NIST Special Publication 800-30, September 2012. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

National Institute of Standards and Technology (NIST), "Guide to Cyber Threat Information Sharing," NIST Special Publication 800-150, October 2016. http://dx.doi.org/10.6028/NIST.SP.800-150

National Institute of Standards and Technology (NIST), "Guide to Industrial Control Systems (ICS) Security," SP 800-82, May 2015. https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final

National Institute of Standards and Technology (NIST), "NIST Risk Management Framework Overview." https://www.nist.gov/system/files/documents/2018/03/28/vickie_nist_risk_management_framework_overview-hpc.pdf

National Institute of Standards and Technology (NIST), "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations," NIST Special Publication 800-171 Rev. 2, February 2020. https://doi.org/10.6028/NIST.SP.800-171r2

Santos, O., "Cisco CyberOps Associate, CBROPS 200-201, Official Cert Guide," December 2020. https://www.ciscopress.com/store/cisco-cyberops-associate-cbrops-200-201-official-cert-9780136807834

U.S. Department of Energy, Cybersecurity Capability Maturity Model (C2M2), September 2021. https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/energy-sector-cybersecurity-0

U.S. Department of Homeland Security CISA, "Cybersecurity Practices for Industrial Control Systems." https://www.cisa.gov/publication/Cybersecurity-Best-Practices-for-Industrial-Control-Systems

U.S. Department of Homeland Security CISA, "Transportation Systems Sector Cybersecurity Framework Implementation Guidance," June 2015. https://www.cisa.gov/sites/default/files/publications/tss-cybersecurity-framework-implementation-guide-2016-508v2_0.pdf

U.S. Department of Homeland Security CISA, "Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies," September 2016. https://www.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf

U.S. Department of Homeland Security National Cyber Security Division, "Public Safety Communications Resiliency," July 2017. https://www.cisa.gov/sites/default/files/publications/07202017_10_Keys_to_Public_Safety_Network_Resiliency_010418_FINAL508C.pdf

Definitions

automatic train protection (ATP): A wayside and/or onboard train system to apply emergency brakes if a signal is missed by the train operator.

automatic train supervision (ATS): Provides advanced functionalities of train control, typically including advanced automatic routing and automatic train regulation.

CISA: The Cybersecurity and Infrastructure Security Agency is a component of the U.S. Department of Homeland Security that leads the national effort to understand, manage and reduce risk to the country's cyber and physical infrastructure.

Cybersecurity Capability Maturity Model (C2M2): A tool for evaluating and improving cybersecurity. It was developed in 2012 by the U.S. energy sector and the Department of Energy. The C2M2 is managed by the DOE's Office of Cybersecurity, Energy Security, and Emergency Response (CESER), Cybersecurity for Energy Delivery Systems (CEDS) division.

communications-based train control (CBTC): A continuous, automatic train control system that relies on wayside data communications and/or GPS for position sensing and uses the "moving block" principle for safe train separation rather than fixed blocks with track circuits.

common operating picture (COP): A continuously updated overview of an incident compiled throughout an incident's life cycle from data shared between integrated communication, information management, and intelligence and information sharing systems.

configuration management: A practice and process of handling hardware, software and firmware changes systematically so a device or system maintains its integrity over time.

cybersecurity: The field of protecting digital computers and networks from accidental or malicious modifications.

Defense-in-Depth: A layered approach to information security that uses multiple computer security techniques to help mitigate the risk of one component of the defense being compromised or circumvented.

electronic security perimeter (ESP): Adapted from NERC-CIP electric power regulations, a logical perimeter drawn around electronic assets in a security zone to separate them from other zones.

emergency cutoff (blue light) system: A safety system installed at passenger stations that cuts off traction power and notifies the control center that power has been cut at this location.

Enterprise Zone: The zone of a transit agency that handles its routine internal business processes and other nonoperational, non-fire-and-life-safety, and non-safety-critical information.

fail-safe: A device that fails in a manner that protects the safety of personnel and equipment.

Fire and Life-Safety Security Zone (FLSZ): A zone containing systems whose primary function is to warn, protect or inform in an emergency. It contains systems such as fire alarms and emergency ventilation.

interlocking: An arrangement of railway signals and signal appliances so interconnected that their movements must succeed one another in proper sequence.

IPSec: A suite of protocols for securing Internet Protocol communications that authenticates and encrypts each IP packet in a communication session.

malware: Short for malicious software. Such software is created and used by people, usually with bad intentions, to disrupt computer operations or obtain, without consent, confidential information.

NIST SP 800-53: NIST Special Publication 800-53, titled “Recommended Security Controls for Federal Information Systems and Organizations” (see “References”). Rev. 5, dated January 2020, was used in preparing this document.

NIST SP 800-82: NIST Special Publication 800-82, titled “Guide to Industrial Control Systems (ICS) Security” (see “References”). The May 2015 final version was used in preparing this document.

Operations Control Center (OCC): A central location that monitors, and in some cases controls, some portion of a transportation system. It may handle just one system or many systems simultaneously.

Operationally Critical Security Zone (OCSZ): A security zone containing systems necessary for proper operation of rail transit, such as SCADA, dispatch and ATS.

patch management: A regular, coordinated method for equipment vendors to update software and firmware fixes for their digital equipment at transit agencies in a timely and responsible manner.

programmable logic controller (PLC): An industrial computer used for automation of mechanical processes.

risk: A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of the adverse impacts that would arise if the circumstance or event occurs and the likelihood of occurrence.

risk management: The process of identifying risk, assessing risk and taking steps to reduce risk to an acceptable level.

Safety Critical Security Zone (SCSZ): The zone that contains vital signaling, interlocking and ATP within rail transit.

SCADA: A control system involving a master terminal unit and remote terminal units, used for supervisory control and data acquisition.

track circuit: An electrical circuit designed to indicate the presence or absence of a train in a specific section of track.

traction power: A network supplying power to electrically powered railways.

trusted (network): Network of an organization that is within the organization's ability to control or manage. Further, it is known that the network's integrity is intact and that no intruder is present.

vector (for cyberattack): The path an attacker takes to attack a network. (This term is borrowed from biology, where disease is traced from its origin through the various carriers and paths taken to infect the victim.)

vital: A term applied within rail safety to denote fail-safe operation. (Derived from IEEE Standard 1483, 2000 glossary, "vital function: A function in a safety-critical system that is required to be implemented in a fail-safe manner.")

vital programmable logic controller (vital PLC): A PLC with fail-safe functions intended for safety-critical signaling and interlocking applications in rail transit.

vital signaling: The portion of a railway signaling network that contains vital equipment.

virtual private network (VPN): A computer network in which some of the connections are virtual circuits instead of direct connections via physical wires within some larger network, such as the internet. A VPN in and of itself is not necessarily secure.

whitelisting: Describes a list or register of entities that are granted certain privileges, services, mobility, access or recognition.

Wi-Fi: In the broadest sense, all short-range communications that use some type of electromagnetic spectrum to send and/or receive information without wires.

Abbreviations and acronyms

AI	artificial intelligence
ATP	automatic train protection
CAN	controller area network
CBTC	communications-based train control
CCSWG	Control and Communications Security Working Group
CIS	Center for Internet Security
CISA	Cybersecurity and Infrastructure Security Agency
COP	common operating picture
CSET	Cyber Security Evaluation Tool
CSF	Cybersecurity Framework
CSO	chief security officer
DHS	U.S. Department of Homeland Security
ECSWG	Enterprise Cybersecurity Working Group
ESP	electronic security perimeter
FIPS	Federal Information Processing Standard
FLSZ	Fire and Life-Safety Security Zone
ICS	industrial control system
ICS-CERT	Industrial Control Systems Computer Emergency Response Team
IEEE	Institute of Electrical and Electronics Engineers (commonly just IEEE)
IPFIX	Internet Protocol Flow Information Export
IPSec	Internet Protocol Security
ISA	International Society of Automation
IT	information technology
KPI	key performance indicator
KRI	key risk indicator
ML	machine learning
MSSP	managed security service provider
NSA	National Security Agency
NERC	North American Electric Reliability Corporation
NERC-CIP	North American Electric Reliability Corporation – Critical Infrastructure Protection
NIST	National Institute of Standards and Technology
OCC	Operations Control Center
OCSZ	Operationally Critical Security Zone
OWASP	Open Web Application Security Project
PLC	programmable logic controller
RMF	Risk Management Framework
SCADA	supervisory control and data acquisition
SCSZ	Safety Critical Security Zone
SDLC	system development life cycle
SIEM	security information and event management
SIPOC	suppliers, inputs, processes, outputs, customers
SOAR	security orchestration, automation and response
SOC	Security Operations Center
ST-ISAC	Surface Transportation Information Sharing and Analysis Center
TCP/IP	Transmission Control Protocol/Internet Protocol
TSA	U.S. Transportation Security Administration
VPN	virtual private network

Document history

Document Version	Working Group Vote	Public Comment/ Technical Oversight	Rail CEO Approval	Policy & Planning Approval	Publish Date
First published	Aug. 17, 2022	Dec. 1, 2022	March 6, 2023	March 31, 2023	May 23, 2023

Appendix A: OT-CMF Maturity Levels

Level 0: Baseline (On-Ramp). Establishes the foundation necessary for developing, implementing, maintaining and maturing a cybersecurity program in a transit organization to include the following:

1. Executive leadership provides a documented policy statement and commitment to supporting the development of a transit control system cybersecurity program.
2. Identify a security champion with authority to drive the cybersecurity program.
3. Identify and document operational technology assets.
4. Identify and create implementation plan for Tier 1 OT-CMF controls.
5. Develop a cybersecurity hygiene and awareness program.
6. Create awareness of known cybersecurity threats across the organization.
7. Perform a cybersecurity self-assessment.

Level 1: Initiated. Builds upon Level 0 as a next step for enhancing, maturing and maintaining a cybersecurity program in an organization. Level 1 requires organizations to do the following:

1. Obtain formal acknowledgment and approval of the adoption of the OT-CMF from executive leadership.
2. Appoint security liaisons across the organization to coordinate cybersecurity program activities in their respective business units.
3. Define and approve the purpose of each operational technology asset.
4. Collaborate with business groups/units across the organization to document security operating procedures and processes.
5. Publicize known cybersecurity threats across the organization.
6. Implement a cybersecurity hygiene and awareness program.
7. Revise and republish the approved procedures and processes to relevant stakeholders.
8. Review the recommended OT-CMF controls and perform a cybersecurity self-assessment on an annual basis.

Level 2: Planned. Builds upon Level 1 to further enhance and mature the organization's control system cybersecurity program. Level 2 requires organizations to do the following:

1. Obtain executive leadership approval for establishing a charter, a Cybersecurity Governance Committee and the appointment of a committee leader.
2. Cybersecurity Governance Committee:
    a. Define the security liaison's roles and responsibilities in coordinating cybersecurity program development and dissemination activities within their business units.
    b. Develop agency-specific policies, procedures and processes aligned to the OT-CMF.
    c. Define the cybersecurity policies and standards for procurement and acquisition.
    d. Develop an OT Risk Management Program and ensure that OT-CMF aligns with the Enterprise Risk Management Program.
    e. Identify key performance indicators and key risk indicators.
    f. Collect and analyze risk data from all control systems to establish risk acceptance criteria.
    g. Establish guidelines and benchmarks for measuring progress and compliance with the OT-CMF.
    h. Develop an organizational control system cybersecurity training and awareness program.
    i. Clearly define service level agreements/operations level agreements.
3. Define and document the OT safety and security zone architecture.
4. Implement agency-selected Tier 2 OT-CMF controls from Level 1.
5. Assess and select Tier 3 OT-CMF controls to be implemented in Level 3.
9. Conduct a cybersecurity self-assessment or engage third parties to perform a cybersecurity assessment.

Level 3: Operationalized. Builds upon Level 2 to further enhance and mature the organization's control system's cybersecurity program. Level 3 requires organizations to do the following:

1. Establish an OT Security Controls Systems Monitoring Program.
2. Establish a continuous improvement program from the metrics as defined in Level 2, Section 5.2.6.
    a. Review and update the recommended controls to align with the agency's security goals and objectives.
3. Identify gaps in policies, procedures and current practices across the organization, and develop remediation strategies to ensure compliance.
4. Enhance policies and supporting operating procedures by developing, documenting, approving and publishing changes organization wide.
5. Define status reporting processes—i.e., to senior management, relevant system owners and stakeholders—of any identified issues.
6. Evaluate operating procedures, identify efficiencies and implement for each OT-CMF domain.
7. Implement a role-based, organization-wide cybersecurity training and threat awareness program.
8. Define classification and risk calculation standards to assess the risk and qualify/quantify the impact.
9. Implement Tier 3 recommended OT-CMF controls identified in Level 2, Section 5.5.
10. Perform a third-party annual audit of the OT cybersecurity program.

Level 4: Managed. Builds upon Level 3 to further enhance the organization's cybersecurity program with standardization and optimization to achieve a higher maturity level. Level 4 requires organizations to do the following:

1. Appoint a cybersecurity professional to the board of directors to oversee the cybersecurity initiatives across the organization.
2. Establish a formal, self-contained cyber-intelligence program with independent analysis capability.
3. Standardize and optimize the established policies, standards and procedures to protect, detect, respond and adapt to the changing threat landscape.
4. Enforce role-based organizational control systems cybersecurity training and awareness for all stakeholders and require certifications.
5. Secure infrastructure design with network segmentation to ensure limited user and device access.
6. Implement security orchestration automation and response (SOAR).
7. Integrate security controls monitoring program with enterprise security information and event management (SIEM).
8. Automate mitigation of vulnerabilities with clearly defined service level agreements/operation level agreements (SLAs/OLAs).
9. Establish processes and technologies to report emerging threats to the board of directors.
11. Engage third parties to perform an annual audit of the operations technology cybersecurity program.

Level 5: Optimized. Builds upon Level 4 to fully mature the organization's cybersecurity program. Level 5 requires organizations to have the following:

1. Security orchestration to monitor, hunt and react to potential zero-day threats and vulnerabilities.
2. Advanced proactive processes with tools and technologies to protect, detect, respond and autonomously adapt to a changing threat landscape.
3. Automated and optimized processes to continuously monitor and improve operations technology cybersecurity controls' efficiency and performance.
4. Real-time reporting of organizational threats and vulnerabilities to senior management.
5. An annual third-party audit of the OT continuous monitoring and automated response system.

Appendix B: OT-CMF controls guidance

This appendix gives guidance for the consideration and implementation of industrial control systems (ICS) and operational technology cybersecurity controls within the OT-CMF framework. There are several outcomes expected from the OT-CMF controls guidance:

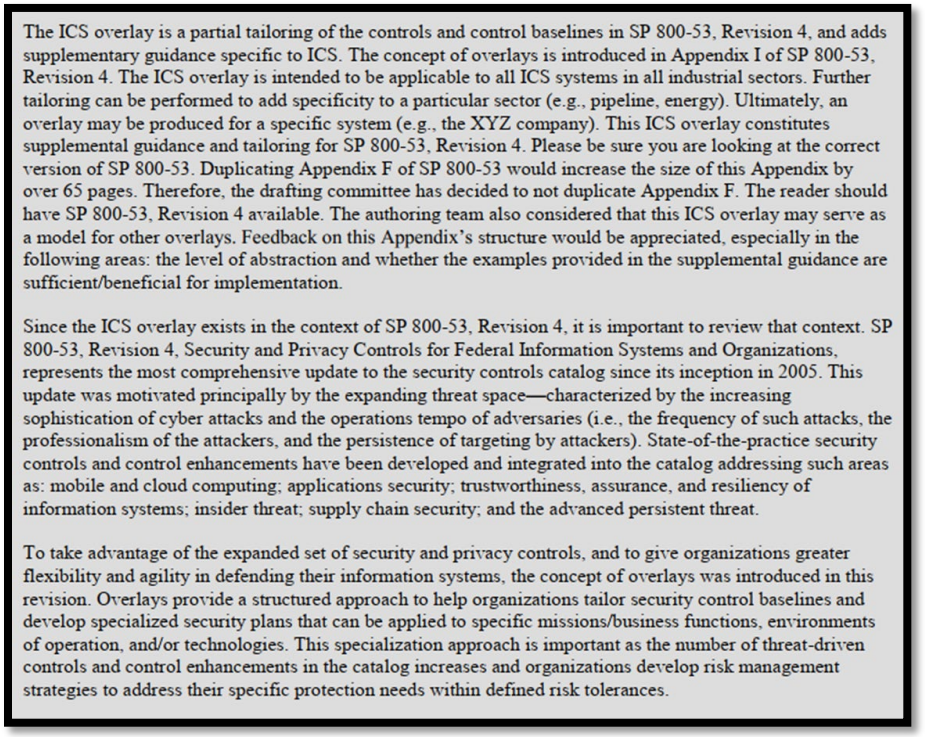
1. Communicate and inform the implementation of critical high-priority controls. These are controls that should be implemented for the operational technology systems of *all* public transportation agencies.
2. Elicit thought-provoking control selection and implementation of second- and third-tier controls. This exercise of reviewing controls for implementation is what allows this controls guidance to be adaptive to the needs of public transportation agencies of any size. The right controls to implement ultimately depend on an agency's mission, scope, risk tolerance, budget and cybersecurity culture.
3. Overlay the prioritized controls with the OT-CMF maturity levels and the NIST Risk Management Framework.

B.1 Control selection using NIST and FIPS

NIST 800-82 Rev. 2, which is an operational technology overlay of NIST 800-53 Rev. 4, provides guidance on how to secure ICS, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as programmable logic controllers (PLCs), while addressing their unique requirements.

NIST 800-53 Rev. 4 allows for technology-specific overlays, the intent of which is allowing adoption and guidance of technology-specific controls. NIST 800-82 Rev. 2 is that overlay for OT systems and is the basis for the OT-CMF selected controls. To furnish support for this overlay, the definition of the NIST 800-82 overlay is provided in **Figure 5**.

FIGURE 5
NIST 800-82 Rev. 2, ICS Overlay



The ICS overlay is a partial tailoring of the controls and control baselines in SP 800-53, Revision 4, and adds supplementary guidance specific to ICS. The concept of overlays is introduced in Appendix I of SP 800-53, Revision 4. The ICS overlay is intended to be applicable to all ICS systems in all industrial sectors. Further tailoring can be performed to add specificity to a particular sector (e.g., pipeline, energy). Ultimately, an overlay may be produced for a specific system (e.g., the XYZ company). This ICS overlay constitutes supplemental guidance and tailoring for SP 800-53, Revision 4. Please be sure you are looking at the correct version of SP 800-53. Duplicating Appendix F of SP 800-53 would increase the size of this Appendix by over 65 pages. Therefore, the drafting committee has decided to not duplicate Appendix F. The reader should have SP 800-53, Revision 4 available. The authoring team also considered that this ICS overlay may serve as a model for other overlays. Feedback on this Appendix's structure would be appreciated, especially in the following areas: the level of abstraction and whether the examples provided in the supplemental guidance are sufficient/beneficial for implementation.

Since the ICS overlay exists in the context of SP 800-53, Revision 4, it is important to review that context. SP 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, represents the most comprehensive update to the security controls catalog since its inception in 2005. This update was motivated principally by the expanding threat space—characterized by the increasing sophistication of cyber attacks and the operations tempo of adversaries (i.e., the frequency of such attacks, the professionalism of the attackers, and the persistence of targeting by attackers). State-of-the-practice security controls and control enhancements have been developed and integrated into the catalog addressing such areas as: mobile and cloud computing; applications security; trustworthiness, assurance, and resiliency of information systems; insider threat; supply chain security; and the advanced persistent threat.

To take advantage of the expanded set of security and privacy controls, and to give organizations greater flexibility and agility in defending their information systems, the concept of overlays was introduced in this revision. Overlays provide a structured approach to help organizations tailor security control baselines and develop specialized security plans that can be applied to specific missions/business functions, environments of operation, and/or technologies. This specialization approach is important as the number of threat-driven controls and control enhancements in the catalog increases and organizations develop risk management strategies to address their specific protection needs within defined risk tolerances.

NIST 800-82 Rev. 2 contains a total of 262 parent and sub-controls. In order to make control adoption manageable for public transit agencies, APTA's Control and Communications Security Working Group is recommending the adoption of NIST 800-82's *Low* Control Baseline, which further prioritizes and down-selects the number of controls to 134. This down-selection was done by NIST using the FIPS 200.

FIPS 200 provides applicability to public transportation:

> In addition to the agencies of the federal government, state, local, and tribal governments, and private sector organizations that compose the critical infrastructure of the United States are encouraged to consider the use of this standard, as appropriate.

B.2 Control prioritization and tiering by APTA

In order to integrate control guidance with the OT-CMF maturity levels, the 134 NIST 800-82 controls were further prioritized into three tiers.

B.2.1 Tier 1: Required controls

These controls are critical foundational controls and should be implemented in whole by all public transportation agencies.

Most of these controls were identified by a joint exercise in 2016 by members of APTA, the Toronto Transit Commission, and the Department of Energy's Idaho National Labs, and defined in APTA published guidance "Securing Control and Communications Systems in Rail Transit Environments, Part IIIb: Protecting the Operationally Critical Security Zone." Due to changes in the threat landscape, several additional controls were added to the Tier 1 controls.

B.2.2 Tier 2 and Tier 3: Controls to be evaluated

The Tier 2 and Tier 3 controls are further prioritized; after significant review and collaboration, the APTA Control and Communications Security Working Group has assigned controls to higher (Tier 2) or lower (Tier 3) groups based on their analyzed efficacy against the cybersecurity threats facing public transportation agencies.

These controls are not prescriptive; they are meant to elicit thought-provoking control evaluation, selection and implementation. This exercise of reviewing controls for implementation is what allows this controls guidance to be adaptive to the needs of public transportation agencies of any size. The right controls to implement ultimately depend on the agency's mission, scope, risk tolerance, budget and cybersecurity culture. They are summarized in **Table 4**.

TABLE 4
OT-CMF Control Tiers

OT-CMF Control Tiers	Description	Number of Controls
Tier 1	Foundational Controls	29
Tier 2	CCSWG Priority 2 Selection	56
Tier 3	CCSWG Priority 3 Selection	38

B.3 Supplemental control implementation information

Depending on the actual control, excellent supplemental OT information can be found in several locations that should be used to inform control selection and implementation. The best source of supplemental

information is identified for each control, located in Section B.5. The sources of information include the following:

- **"Securing Control and Communications Systems in Rail Transit Environments, Part IIIb: Protecting the Operationally Critical Security Zone."** This APTA document offers excellent and practical descriptions of its controls, including additional references and supplementary information.
- **NIST 800-82 Rev. 2, "Guide to Industrial Control Systems (ICS) Security."** The purpose of NIST 800-82 is to provide guidance for securing ICS, including SCADA and DCS systems, PLCs, and other systems performing industrial control functions. In many cases it provides ICS control enhancements to NIST 800-53 Rev. 4 controls by providing additional ICS supplemental guidance and ICS control tailoring. **Figure 6** shows how additional ICS context is provided to an 800-53 Rev. 4 control:

FIGURE 6
NIST 800-82 Rev. 2 Example: ICS Supplemental Information

SI-4 INFORMATION SYSTEM MONITORING

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SI-4	**Information System Monitoring**	Selected	Selected	Selected
SI-4 (2)	*INFORMATION SYSTEM MONITORING | AUTOMATED TOOLS FOR REAL-TIME ANALYSIS*		Selected	Selected
SI-4 (4)	*INFORMATION SYSTEM MONITORING | INBOUND AND OUTBOUND COMMUNICATIONS TRAFFIC*		Selected	Selected
SI-4 (5)	*INFORMATION SYSTEM MONITORING | SYSTEM-GENERATED ALERTS*		Selected	Selected

ICS Supplemental Guidance: The organization ensures that the use of monitoring tools and techniques does not adversely impact the operational performance of the ICS. Example compensating controls include deploying sufficient network monitoring.

Control Enhancement: (2) ICS Supplemental Guidance: In situations where the ICS cannot support the use of automated tools to support near-real-time analysis of events, the organization employs compensating controls (e.g., providing an auditing capability on a separate system, nonautomated mechanisms or procedures) in accordance with the general tailoring guidance.

Control Enhancement: (4) ICS Supplemental Guidance: In situations where the ICS cannot monitor inbound and outbound communications traffic, the organization employs compensating controls include providing a monitoring capability on a separate information system.

Control Enhancement: (5) ICS Supplemental Guidance: Example compensating controls include manual methods of generating alerts.

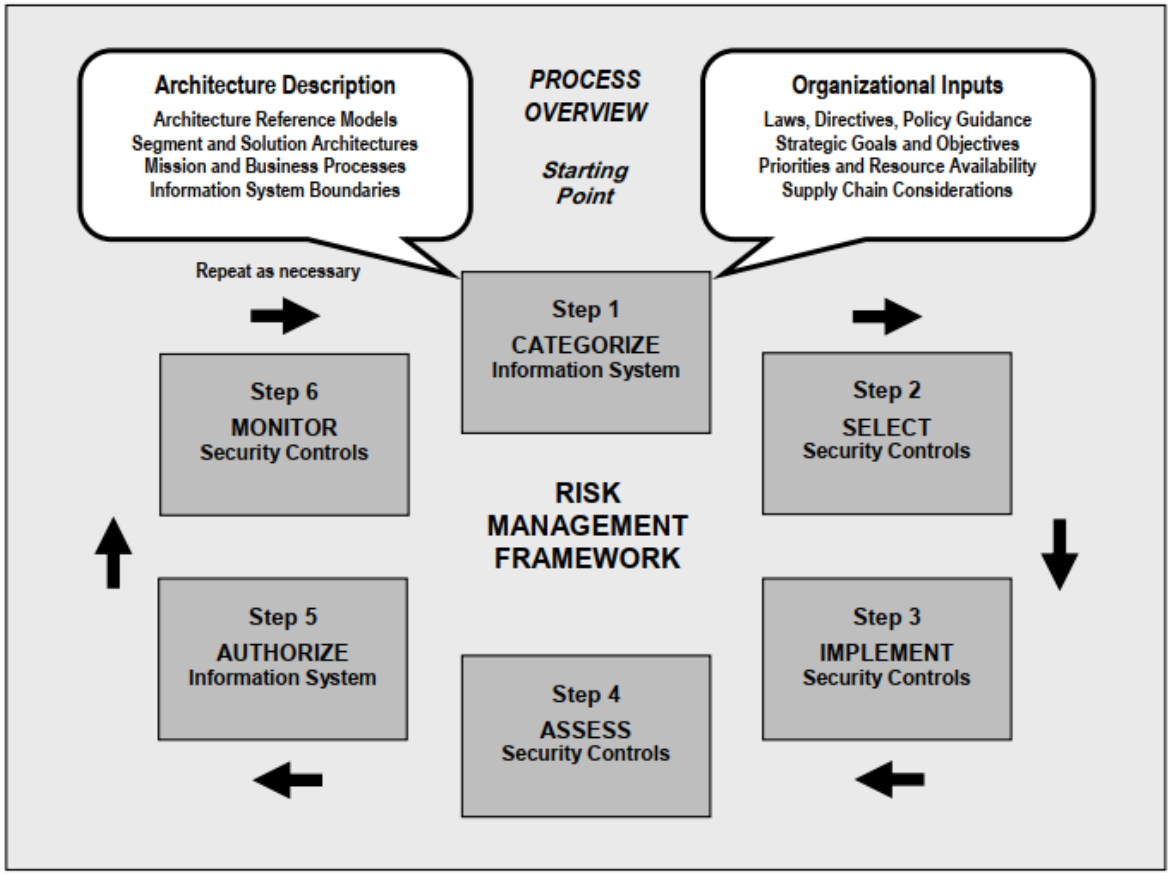
Many controls do not necessarily need to be tailored to an ICS environment. In these cases, control guidance can be found in NIST 800-53 Rev. 4.

B.4 Integration of control guidance with OT-CMF and the NIST RMF

B.4.1 NIST Risk Management Framework overview

NIST 800-37 Rev. 2, the Risk Management Framework (RMF), provides a disciplined, structured and flexible process for managing security and privacy risk that includes information security categorization; control selection, implementation and assessment; system and common control authorizations; and continuous monitoring. APTA's CCSWG recommends referencing and using the RMF for managing the life cycle of control for OT systems. **Figure 7** depicts the RMF as it relates to ICS controls.

FIGURE 7
NIST 800-37 Rev. 2: Executing the RMF Tasks for Industrial Control Systems



B.4.2 Integration of OT-CMF levels, OT-CMF controls and NIST RMF

Since OT-CMF control guidance is leveraging NIST controls, it is important to understand the relationship between the OT-CMF maturity levels, control tiers and the NIST Risk Management Framework. **Table 5** outlines the relationship between these guiding standards.

TABLE 5
OT-CMF Control Relationships

OT-CMF Maturity Level	NIST Risk Management Framework	OT-CMF Control Tiers
CCSWG Development	Categorize	
Level 0: Baseline	Identify	Tier 1
Level 1: Initiated	Implement Assess / Select	Tier 1 Tier 2
Level 2: Planned	Implement/Authorize Assess/Select	Tier 2 Tier 3
Level 3: Operationalized	Implement/Authorize Assess/Select	Tier 3 Agency-specific
Level 4: Managed	Monitor → Select → Implement → Assess → Authorize	Agency-specific
Level 5: Optimized	N/A	

B.5 OT-CMF Controls

TABLE 6
OT-CMF Controls, Tier 1

NIST 800-53 Reference Control (Sub-Control)	Control Name	Hyperlink to Recommended Control Guidance	Page #
AC-17	Remote Access	https://www.apta.com/wp-content/uploads/Standards_Documents/APTA-SS-CCS-RP-004-16.pdf	29
AC-18	Wireless Access	https://www.apta.com/wp-content/uploads/Standards_Documents/APTA-SS-CCS-RP-004-16.pdf	24,32
AC-2	Account Management	https://www.apta.com/wp-content/uploads/Standards_Documents/APTA-SS-CCS-RP-004-16.pdf	30
AT-1	Security Awareness and Training Policy and Procedures	https://www.apta.com/wp-content/uploads/Standards_Documents/APTA-SS-CCS-RP-004-16.pdf	18
AU-1	Audit and Accountability Policy and Procedures	https://www.apta.com/wp-content/uploads/Standards_Documents/APTA-SS-CCS-RP-004-16.pdf	30
AU-12	Audit Generation	https://www.apta.com/wp-content/uploads/Standards_Documents/APTA-SS-CCS-RP-004-16.pdf	25
CA-2	Security Assessments	https://www.apta.com/wp-content/uploads/Standards_Documents/APTA-SS-CCS-RP-004-16.pdf	17
CA-6	Security Authorization	https://www.apta.com/wp-content/uploads/Standards_Documents/APTA-SS-CCS-RP-004-16.pdf	17, 31
CM-1	Configuration Management Policy and Procedures	https://www.apta.com/wp-content/uploads/Standards_Documents/APTA-SS-CCS-RP-004-16.pdf	20
CM-2	Baseline Configuration	https://www.apta.com/wp-content/uploads/Standards_Documents/APTA-SS-CCS-RP-004-16.pdf	20
CM-3	Configuration Change Control	https://www.apta.com/wp-content/uploads/Standards_Documents/APTA-SS-CCS-RP-004-16.pdf	21
CM-7 incl. (1)	Least Functionality	https://www.apta.com/wp-content/uploads/Standards_Documents/APTA-SS-CCS-RP-004-16.pdf	23
CM-8	Information System Component Inventory	https://www.apta.com/wp-content/uploads/Standards_Documents/APTA-SS-CCS-RP-004-16.pdf	21
CP-2	Contingency Plan	https://www.apta.com/wp-content/uploads/Standards_Documents/APTA-SS-CCS-RP-004-16.pdf	27
CP-4	Contingency Plan Testing	https://www.apta.com/wp-content/uploads/Standards_Documents/APTA-SS-CCS-RP-004-16.pdf	27
IR-1	Incident Response Policy and Procedures	https://www.apta.com/wp-content/uploads/Standards_Documents/APTA-SS-CCS-RP-004-16.pdf	34
MA-4	Nonlocal Maintenance	https://www.apta.com/wp-content/uploads/Standards_Documents/APTA-SS-CCS-RP-004-16.pdf	16
PE-1	Physical and Environmental Protection Policy and Procedures	https://www.apta.com/wp-content/uploads/Standards_Documents/APTA-SS-CCS-RP-004-16.pdf	19
PS-4	Personnel Termination	https://www.apta.com/wp-content/uploads/Standards_Documents/APTA-SS-CCS-RP-004-16.pdf	18
SA-1	System and Services Acquisition Policy and Procedures	https://www.apta.com/wp-content/uploads/Standards_Documents/APTA-SS-CCS-RP-004-16.pdf	22

TABLE 6
OT-CMF Controls, Tier 1

NIST 800-53 Reference Control (Sub-Control)	Control Name	Hyperlink to Recommended Control Guidance	Page #
SA-4 incl. (10)	Acquisition Process	https://www.apta.com/wp-content/uploads/Standards_Documents/APTA-SS-CCS-RP-004-16.pdf	22
SC-41	Port and I/O Device Access	https://www.apta.com/wp-content/uploads/Standards_Documents/APTA-SS-CCS-RP-004-16.pdf	23
SC-7	Boundary Protection	https://www.apta.com/wp-content/uploads/Standards_Documents/APTA-SS-CCS-RP-004-16.pdf	12–15
SI-17	Fail-Safe Procedures	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf	G-64
SI-2	Flaw Remediation	https://www.apta.com/wp-content/uploads/Standards_Documents/APTA-SS-CCS-RP-004-16.pdf	27
SI-3	Malicious Code Protection	https://www.apta.com/wp-content/uploads/Standards_Documents/APTA-SS-CCS-RP-004-16.pdf	23-26
SI-4	Information System Monitoring	https://www.apta.com/wp-content/uploads/Standards_Documents/APTA-SS-CCS-RP-004-16.pdf	24
SI-5	Security Alerts, Advisories, and Directives	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf	G-61
SI-7	Software, Firmware, and Information Integrity	https://www.apta.com/wp-content/uploads/Standards_Documents/APTA-SS-CCS-RP-004-16.pdf	33,34

TABLE 7
OT-CMF Controls, Tier 2

NIST 800-53 Reference Control (Sub-Control)	Control Name	Hyperlink to Recommended Control Guidance	Page #
AC-1	Access Control Policy and Procedures	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf	G-14
AC-14	Permitted Actions without Identification or Authentication	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf	44
AC-19	Access Control for Mobile Devices	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf	G-18
AC-20	Use of External Information Systems	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf	G-18
AC-22	Publicly Accessible Content	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf	G-19
AC-3	Access Enforcement	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf	G-15
AC-7	Unsuccessful Logon Attempts	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf	G-16
AT-2	Security Awareness Training	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf	G-20
AT-3	Role-Based Security Training	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf	G-20

TABLE 7
OT-CMF Controls, Tier 2

NIST 800-53 Reference Control (Sub-Control)	Control Name	Hyperlink to Recommended Control Guidance	Page #
AU-11	Audit Record Retention	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf	77
AU-2	Audit Events	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf	G-21
AU-3	Content of Audit Records	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf	G-21
AU-4 incl. (1)	Audit Storage Capacity	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf	G-21
AU-6	Audit Review, Analysis, and Reporting	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf	70
AU-8	Time Stamps	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf	G-22
CA-1	Security Assessment and Authorization Policies and Procedures	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf	G-24
CA-3	System Interconnections	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf	G-24
CA-5	Plan of Action and Milestones	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf	88
CA-7	Continuous Monitoring	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf	G-25
CA-9	Internal System Connections	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf	G-26
CM-11	User-Installed Software	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf	112
CM-4	Security Impact Analysis	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf	G-27
CM-6	Configuration Settings	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf	103
CP-10	Information System Recovery and Reconstitution	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf	G-32
CP-3	Contingency Training	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf	118
CP-9	Information System Backup	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf	125
IA-1	Identification and Authentication Policy and Procedures	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf	G-33
IA-2 incl. (1) (12)	Identification and Authentication (Organizational Users)	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf	G-33
IA-3	Device Identification and Authentication	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf	G-34
IA-4	Identifier Management	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf	136

TABLE 7
OT-CMF Controls, Tier 2

NIST 800-53 Reference Control (Sub-Control)	Control Name	Hyperlink to Recommended Control Guidance	Page #
IA-8 incl. (1) (2) (3) (4)	Identification and Authentication (Non Organizational Users)	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf	G-35
IR-2	Incident Response Training	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf	150
IR-4	Incident Handling	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf	152
IR-5	Incident Monitoring	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf	156
IR-6	Incident Reporting	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf	G-37
IR-7	Incident Response Assistance	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf	158
IR-8	Incident Response Plan	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf	158
PE-11 incl. (1)	Emergency Power	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf	G-44
PE-13	Fire Protection	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf	G-45
PE-14	Temperature and Humidity Controls	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf	189
PE-15	Water Damage Protection	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf	G-45
PS-5	Personnel Transfer	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf	225
RA-1	Risk Assessment Policy and Procedures	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf	G-51
RA-2	Security Categorization	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf	239
RA-3	Risk Assessment	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf	240
RA-5	Vulnerability Scanning	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf	G-51
SA-3	System Development Life Cycle	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf	250
SA-5	Information System Documentation	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf	256
SA-9	External Information System Services	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf	271
SC-1	System and Communications Protection Policy and Procedures	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf	G-55
SC-12	Cryptographic Key Establishment and Management	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf	G-57

TABLE 7
OT-CMF Controls, Tier 2

NIST 800-53 Reference Control (Sub-Control)	Control Name	Hyperlink to Recommended Control Guidance	Page #
SC-13	Cryptographic Protection	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf	308
SC-21	Secure Name /Address Resolution Service (Recursive or Caching Resolver)	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf	313
SC-39	Process Isolation	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf	G-59
SC-5	Denial of Service Protection	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf	G-56
SI-1	System and Information Integrity Policy and Procedures	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf	G-60