Transportation Management Center Information Technology Security

Final Report

September 2019

U.S. Department of Transportation
Federal Highway Administration

The Federal Highway Administration (FHWA) Office of Operations (HOP) is pleased to present this guide on Transportation Management Center (TMC) Information Technology (IT) Security.

TMCs and Intelligent Transportation System (ITS) infrastructure are designed with technologies such as Ethernet IP-enabled networks and wireless connectivity capabilities. While such technologies are designed to provide needed communications to support transportation management and operations, the advancements in communications technology result in TMCs and ITS devices no longer functioning as closed systems, thus increasing the e-enabled threats and risks to these transportation facilities and infrastructure. This report serves as technical guidelines for TMCs on improving IT security for their facilities, networks, workstations, servers, data storage, peripherals, and operations. The report will help agencies in mitigating the risks from cyber-attacks on the TMCs and associated servers, peripherals and communications network infrastructure. The report offers recommended strategies and actions to address both short term and long term issues.

This publication's status is: final.

Notice

This document is disseminated under the sponsorship of the U.S. Department of Transportation in the interest of information exchange. The U.S. Government assumes no liability for the use of the information contained in this document.

The U.S. Government does not endorse products or manufacturers. Trademarks or manufacturers' names appear in this report only because they are considered essential to the objective of the document.

Quality Assurance Statement

The Federal Highway Administration (FHWA) provides high-quality information to serve Government, industry, and the public in a manner that promotes public understanding. Standards and policies are used to ensure and maximize the quality, objectivity, utility, and integrity of its information. The FHWA periodically reviews quality issues and adjusts its programs and processes to ensure continuous quality improvement.

Technical Report Documentation Page

1. Report No.

FHWA-HOP-19-059

2. Government Accession No.

3. Recipient's Catalog No.

4. Title and Subtitle

Transportation Management Center Information Technology Security

5. Report Date

September 2019

6. Performing Organization Code

7. Author(s)

Alan Toppen, Jon Chambers, Armand Ciccarelli, Laura Gomez-Martin, Chris Daywalt, Kodi Berger

8. Performing Organization Report No.

9. Performing Organization Name and Address

Kimley-Horn, Reston, Virginia
Skyline Technology Solutions, Glen Burnie, Maryland

Under Contract to:

Cambridge Systematics, Inc.
3 Bethesda Metro Center, Suite 1200
Bethesda, MD 20814

10. Work Unit No. (TRAIS)

11. Contract or Grant No.

DTFH61-16-D-00051

12. Sponsoring Agency Name and Address

U.S. Department of Transportation
Federal Highway Administration
Office of Operations (HOP)
1200 New Jersey Avenue SE
Washington, DC 20590

13. Type of Report and Period Covered

Final Report

14. Sponsoring Agency Code

HOP

15. Supplementary Notes

Task Order Contracting Officer's Representative (TOCOR) – Jimmy Chu

16. Abstract

Cybersecurity is a growing concern worldwide. Over the past several years, much focus has been placed on critical infrastructure providers and their ability to implement cybersecurity in order to continue providing critical services. Traffic Management Centers (TMCs) and Intelligent Transportation Systems (ITS) infrastructure leverage modern communications systems to support transportation management and operations. As a result, TMCs and ITS devices no longer function as closed systems, thus increasing the risk of cyber threats to these transportation facilities and infrastructure.

This report has been developed based on best practices within the industry to reflect the reality within TMCs, while pushing for improvements where necessary with a primary focus on the NIST (National Institute of Standards and Technology) Cybersecurity Framework and CIS (Center for Internet Security) Top 20 Controls. Through this report, TMCs will gain insight into basic practices that serve as a starting point or baseline for organizations with limited resources and cybersecurity expertise, as well as guidelines for TMCs looking to increase their system maturity.

17. Key Words

Cybersecurity, internet, traffic management centers, standards, technology

18. Distribution Statement

No restrictions

19. Security Classif. (of this report)

Unclassified

20. Security Classif. (of this page)

Unclassified

21. No. of Pages

126

22. Price

N/A

SI* (MODERN METRIC) CONVERSION FACTORS

APPROXIMATE CONVERSIONS TO SI UNITS

SYMBOL	WHEN YOU KNOW	MULTIPLY BY	TO FIND	SYMBOL
LENGTH				
in	inches	25.4	millimeters	mm
ft	feet	0.305	meters	m
yd	yards	0.914	meters	m
mi	miles	1.61	kilometers	km
AREA				
in^2	square inches	645.2	square millimeters	mm^2
ft^2	square feet	0.093	square meters	m^2
yd^2	square yard	0.836	square meters	m^2
ac	acres	0.405	hectares	ha
mi^2	square miles	2.59	square kilometers	km^2
VOLUME				
fl oz	fluid ounces	29.57	milliliters	mL
gal	gallons	3.785	liters	L
ft^3	cubic feet	0.028	cubic meters	m^3
yd^3	cubic yards	0.765	cubic meters	m^3
NOTE: volumes greater than 1000 L shall be shown in m^3				
MASS				
oz	ounces	28.35	grams	g
lb	pounds	0.454	kilograms	kg
T	short tons (2000 lb)	0.907	megagrams (or "metric ton")	Mg (or "t")
TEMPERATURE (exact degrees)				
°F	Fahrenheit	5 (F-32)/9 or (F-32)/1.8	Celsius	°C
ILLUMINATION				
fc	foot-candles	10.76	lux	lx
fl	foot-Lamberts	3.426	candela/m^2	cd/m^2
FORCE and PRESSURE or STRESS				
lbf	poundforce	4.45	newtons	N
lbf/in^2	poundforce per square inch	6.89	kilopascals	kPa

APPROXIMATE CONVERSIONS FROM SI UNITS

SYMBOL	WHEN YOU KNOW	MULTIPLY BY	TO FIND	SYMBOL
LENGTH				
mm	millimeters	0.039	inches	in
m	meters	3.28	feet	ft
m	meters	1.09	yards	yd
km	kilometers	0.621	miles	mi
AREA				
mm^2	square millimeters	0.0016	square inches	in^2
m^2	square meters	10.764	square feet	ft^2
m^2	square meters	1.195	square yards	yd^2
ha	hectares	2.47	acres	ac
km^2	square kilometers	0.386	square miles	mi^2
VOLUME				
mL	milliliters	0.034	fluid ounces	fl oz
L	liters	0.264	gallons	gal
m^3	cubic meters	35.314	cubic feet	ft^3
m^3	cubic meters	1.307	cubic yards	yd^3
MASS				
g	grams	0.035	ounces	oz
kg	kilograms	2.202	pounds	lb
Mg (or "t")	megagrams (or "metric ton")	1.103	short tons (2000 lb)	T
TEMPERATURE (exact degrees)				
°C	Celsius	1.8C+32	Fahrenheit	°F
ILLUMINATION				
lx	lux	0.0929	foot-candles	fc
cd/m^2	candela/m^2	0.2919	foot-Lamberts	fl
FORCE and PRESSURE or STRESS				
N	newtons	0.225	poundforce	lbf
kPa	kilopascals	0.145	poundforce per square inch	lbf/in^2

*SI is the symbol for the International System of Units. Appropriate rounding should be made to comply with Section 4 of ASTM E380. (Revised March 2003)

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ACRONYMS

ACL	Access Control List
ATO	Authority to Operate
ASLR	Address Space Layout Randomization
AVL	Automatic Vehicle Location
BIA	Business Impact Analysis
BYOD	bring-your-own-devices
CERT	Computer Emergency Response Teams
CIS	Center for Internet Security
CISA	Cybersecurity and Infrastructure Security Agency
CRR	Cybersecurity Resilience Reviews
CSC	Critical Security Controls
CSF	Cybersecurity Framework
DEP	Data Execution Prevention
DHCP	Dynamic Host Configuration Protocol
DHS	Department of Homeland Security
DLP	data loss prevention
DMARC	Domain-based Message Authentication, Reporting and Conformance
DMS	Dynamic Message Signs
DMZ	Demilitarized Zone
DNS	Domain Name System
DOT	Department of Transportation
EU	the European Union
FIPS	Federal Information Processing Standards
FOIA	Freedom of Information Act
FTP	File Transfer Protocol
GDPR	General Data Protection Regulation
HAR	Highway Advisory Radio
HTTP	Hypertext Transfer Protocol
IaaS	Infrastructure as a Service
IANA	Internet Assigned Numbers Authority
ICS	Industrial Control Systems
IFB	Invitation for Bid
IoT	Internet of Things
IPS	Intrusion Prevention Systems
IRM	Information Rights Management
ISAC	Information Sharing and Analysis Centers
ITS	Intelligent Transportation System
LAN	Local Area Network
LCS	Lane Control Signs
LLC	Limited Liability Company
LMS	Learning Management System
MAC	Media Access Control
MFA	Multi-Factor Authentication

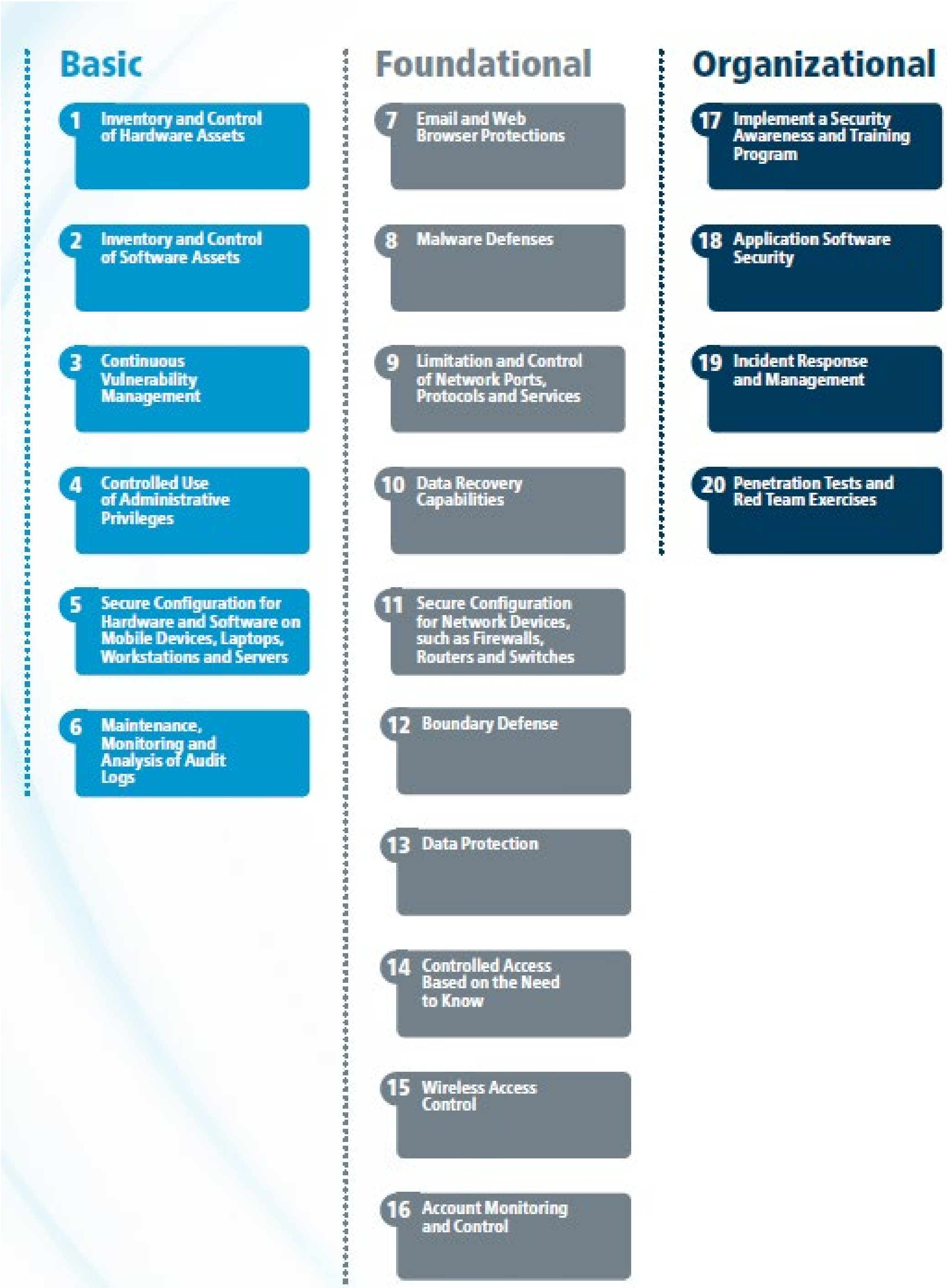
MIL	Maturity Indicator Level
NAC	Network Access Control
NCC-SWG	NIST's Cloud Computing Security Working Group
NCI	National Council of ISACs
NERC	North American Electric Reliability Corporation
NICCS	National Initiative for Cybersecurity Careers and Studies
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
OPSEC	Operational Security
OS	Operating System
OT	Operations Technology
PaaS	Platform as a Service
PCI-DSS	Payment Card Industry Data Security Standards
RDP	Remote Desktop Protocol
RMF	Risk Management Framework
RPO	Recovery Point Objective
RSS	Really Simple Syndication
RTO	Recovery Time Objective
SaaS	Software as a Service
SCADA	Supervisory Control and Data Acquisition
SCAP	Security Content Automation Protocol
SIEM	Security Information and Event Management
SNMP	Simple Network Management Protocol
SP	Special Publication
SPF	Sender Policy Framework
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TMC	Traffic Management Center
UDP	User Datagram Protocol
URL	Uniform Resource Locator
USB	Universal Serial Bus
V2I	Vehicle-to-Infrastructure
VLAN	Virtual Local Access Network
VM	Virtual Machines
VPN	Virtual Private Network
WAF	Web Application Firewalls
WIDS	Wireless Intrusion Detection System
WLAN	Wireless Local Area Network

EXECUTIVE SUMMARY

Cybersecurity is a growing concern worldwide. Over the past several years, much focus has been placed on critical infrastructure providers and their ability to implement cybersecurity in order to continue providing critical services. The Department of Homeland Security considers the Transportation Systems Sector to be 1 of 16 critical infrastructure sectors whose “assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.” The cybersecurity threat landscape is constantly evolving, and new vulnerabilities are discovered every day. Connectivity between different networks, organizations and devices, through the Internet of Things (IoT), further increase exposure to these vulnerabilities.

The material within this report has been developed based on best practices (chapter 3) within the industry that correspond to what Traffic Management Centers (TMC) face on a routine basis, pushing for improvements where necessary, and with a primary focus on the National Institute of Standards and Technology (NIST) Cybersecurity Framework and Center for Internet Security (CIS) Top 20 Controls version 7.1. Through this report, TMCs will gain insight into basic practices that all TMCs should adopt as a starting point or baseline for organizations with limited resources and cybersecurity expertise, as well as guidelines for TMCs looking to increase their system maturity. This report also includes guidelines relevant to personnel controls and elements associated with insider vulnerabilities, and covers controls associated with data protection and resiliency. In chapter 3, an assessment of best practices from TMC operators around the country have been summarized and compared with relevant CIS Top 20 Controls. Additionally, areas of needed improvement have been noted based on controls and policies that are not as mature within the TMC industry.

While synthesizing the available resources on Information Technology (IT) cybersecurity, sources from the Department of Homeland Security (DHS), CIS, and NIST were considered for their relevance to TMCs. The NIST Cybersecurity and Risk Management Frameworks were more abstract and strategic in nature, while the CIS Top 20 Controls provide more technical detailed guidelines of immediate benefit to TMC operators. Therefore, using the CIS Top 20 Controls in baselining security measures provides an immediate impact on guiding control of hardware, software and networks in the TMC, while the NIST frameworks can play a beneficial role to supplement with strategic visioning of Risk Management Plans and Resiliency Plans. The following figure depicts the control framework associated with the CIS Top 20 Controls, which have been identified to be the most relevant for TMCs among the reviewed frameworks.



Basic

1 Inventory and Control of Hardware Assets

2 Inventory and Control of Software Assets

3 Continuous Vulnerability Management

4 Controlled Use of Administrative Privileges

5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

6 Maintenance, Monitoring and Analysis of Audit Logs

Foundational

7 Email and Web Browser Protections

8 Malware Defenses

9 Limitation and Control of Network Ports, Protocols and Services

10 Data Recovery Capabilities

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

12 Boundary Defense

13 Data Protection

14 Controlled Access Based on the Need to Know

15 Wireless Access Control

16 Account Monitoring and Control

Organizational

17 Implement a Security Awareness and Training Program

18 Application Software Security

19 Incident Response and Management

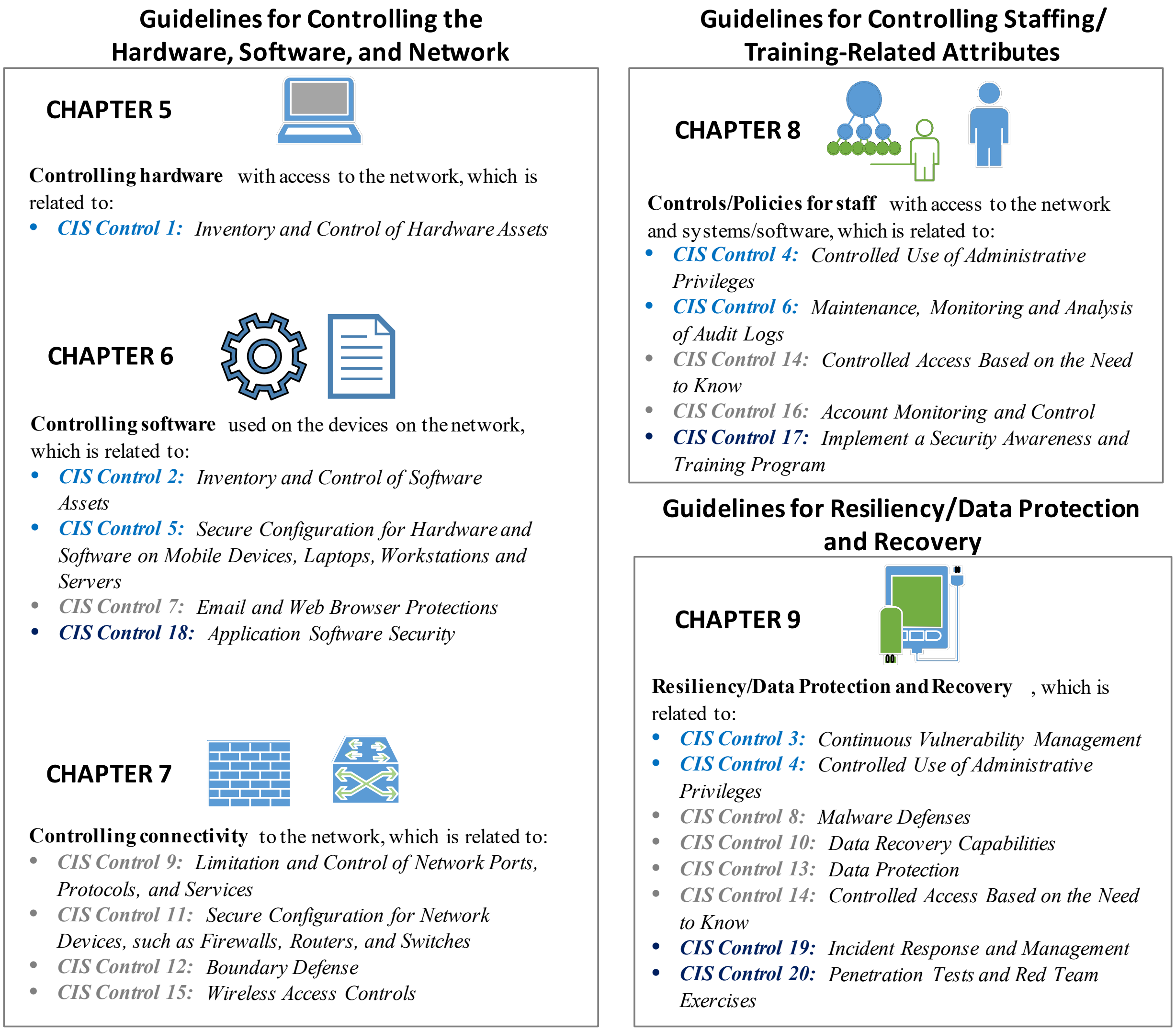
20 Penetration Tests and Red Team Exercises

Figure 1. Chart. Center for Internet Security top 20 critical security controls version 7.1. (Source: CIS Controls Version 7.1.)

The CIS Top 20 Controls are the primary focus of the balance of these guidelines and are discussed in context of applicability to TMC roles. A TMC environment, along with supporting staff, is typically comprised of individuals with distinct roles focused on managing three areas:

- Information technology/systems (subdivided to address networking, devices, hardware, and software).
- Personnel (i.e., human resources).
- Administrative and contractual data management practices (e.g., Freedom of Information Act (FOIA) requests, data archival and organizational resiliency, etc.).

The CIS Top 20 Critical Security Controls correspond to these three functional areas, and each CIS sub-control is relevant to one of the three TMC roles, illustrated in the figure below. They have been color-coded to match the ***Basic***, ***Foundational***, and ***Organizational*** control labeling in the CIS document figures.



Guidelines for Controlling the Hardware, Software, and Network

CHAPTER 5

Controlling hardware with access to the network, which is related to:

- *CIS Control 1: Inventory and Control of Hardware Assets*

CHAPTER 6

Controlling software used on the devices on the network, which is related to:

- *CIS Control 2: Inventory and Control of Software Assets*
- *CIS Control 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers*
- *CIS Control 7: Email and Web Browser Protections*
- *CIS Control 18: Application Software Security*

CHAPTER 7

Controlling connectivity to the network, which is related to:

- *CIS Control 9: Limitation and Control of Network Ports, Protocols, and Services*
- *CIS Control 11: Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches*
- *CIS Control 12: Boundary Defense*
- *CIS Control 15: Wireless Access Controls*

Guidelines for Controlling Staffing/ Training-Related Attributes

CHAPTER 8

Controls/Policies for staff with access to the network and systems/software, which is related to:

- *CIS Control 4: Controlled Use of Administrative Privileges*
- *CIS Control 6: Maintenance, Monitoring and Analysis of Audit Logs*
- *CIS Control 14: Controlled Access Based on the Need to Know*
- *CIS Control 16: Account Monitoring and Control*
- *CIS Control 17: Implement a Security Awareness and Training Program*

Guidelines for Resiliency/Data Protection and Recovery

CHAPTER 9

Resiliency/Data Protection and Recovery , which is related to:

- *CIS Control 3: Continuous Vulnerability Management*
- *CIS Control 4: Controlled Use of Administrative Privileges*
- *CIS Control 8: Malware Defenses*
- *CIS Control 10: Data Recovery Capabilities*
- *CIS Control 13: Data Protection*
- *CIS Control 14: Controlled Access Based on the Need to Know*
- *CIS Control 19: Incident Response and Management*
- *CIS Control 20: Penetration Tests and Red Team Exercises*

Figure 2. Chart. Relationship between Center for Internet Security Controls and Traffic Management Center roles.
(Source: Federal Highway Administration.)

The focus areas of each chapter of this document is depicted in the figure above. Chapter 5 emphasizes elements of controlling hardware with access to the network, while chapters 6 and 7 focus on controlling software and network connectivity, respectively. Chapter 8 focuses primarily on personnel and account privileges/controls, and chapter 9 covers the CIS Controls that address improving resiliency and data protection aspects of TMC IT and Operations.

Following the discussion of the Guidelines, chapter 10 presents recommended short- and long-term strategies for implementation such as conducting a self-assessment Cybersecurity Resilience Reviews (CRR) using DHS' CRR tools, conducting a risk analysis, and implementation Basic and Foundational controls to address the immediate risks identified.

Chapter 11 identifies some key conclusions and next steps recognizing that TMCs around the Nation will be at differing levels of maturity. Some agencies already will have a jumpstart on cybersecurity issues, while others may be closer to starting from scratch when reading these guidelines. If an agency is starting from scratch, a Risk Analysis is recommended as the first step towards establishing a cybersecurity program for the TMC. In conjunction with addressing immediate risks from the Risk Analysis, TMC agencies will benefit from developing a *Risk Management Plan*, as noted in chapter 9, to determine courses of action to mitigate and systematically manage those risks.

Part of increasing the cybersecurity maturity of an agency involves incrementally building a more robust process/program for resiliency by developing a *Resiliency Plan* to harden systems and facilities to improve the ability to recover from an attack or breach.

Finally, TMC operations staff are encouraged to collaborate on the risk analysis with IT staff. The cooperative panel of Operations Technology (OT) and IT staff should lead the charge on routinely testing and improving the program to address existing and newly identified risks. The panel is encouraged to participate in/with peer groups (i.e., Information Sharing and Analysis Centers (ISAC) as noted in chapter 9) to share and learn from identified threats/risks within the TMC community to allow all TMC operators to learn and benefit from the greater body of knowledge.

CHAPTER 1. INTRODUCTION

Cybersecurity is a growing concern worldwide. Over the past several years, much focus has been placed on critical infrastructure providers and their ability to implement cybersecurity in order to continue providing critical services. The Department of Homeland Security considers the Transportation Systems Sector to be 1 of 16 critical infrastructure sectors whose "assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.[1]" The cybersecurity threat landscape is constantly evolving and new vulnerabilities are discovered every day. Connectivity between different networks, organizations and devices, through the Internet of Things (IoT), further increase exposure to these vulnerabilities.

In particular, Traffic Management Centers (TMC) and Intelligent Transportation Systems (ITS) infrastructure leverage modern communications systems to support transportation management and operations. As a result, TMCs and ITS devices no longer function as closed systems, thus increasing the risk of exposure to cyber threats to these transportation facilities and infrastructure. Today's TMCs are often not only automated but also highly integrated. Information Technology (IT) security for TMCs is further complicated by a variety of stakeholders with diverse skillsets and goals, including manufacturers and vendors of system hardware, software and control units; contractors and integrators; and IT specialists with an increasing variety of specialties (e.g., fiber optics, wireless communications, database experts, software integrators, etc.). Thus, it is necessary to research potential IT security threats and solutions for TMCs, and to develop technical guidelines with recommended strategies and actions that agencies should follow to protect those systems and properly respond to the threats.

TMCs can benefit from the practices, experience and lessons learned from IT and other industries that have a wealth of knowledge and experience in mitigating and responding to IT security attacks.

The material within this report has been developed based on best practices within the industry that correspond to what TMCs face on a routine basis, pushing for improvements where necessary, and with a primary focus on the National Institute of Standards and Technology (NIST) Cybersecurity Framework and the Center for Internet Security (CIS) Top 20 Controls version 7.1. Through this report, TMCs will gain insight into basic practices that all TMCs should adopt as a starting point or baseline for organizations with limited resources and cybersecurity expertise, as well as guidelines for TMCs looking to increase their system maturity.

[1] Department of Homeland Security (DHS), "Critical Infrastructure Sectors," 2013. Retrieved from: https://www.dhs.gov/cisa/critical-infrastructure-sectors

CHAPTER 2. CRITICAL TRAFFIC MANAGEMENT CENTERS ELEMENTS

An important aspect of cybersecurity frameworks is that both devices and personnel must be secured. Both the National Institute of Standards and Technology (NIST) Cybersecurity Framework and the Center for Internet Security (CIS) Top 20 Controls underscore this importance.[2,3] In the Traffic Management Center (TMC) context, this involves identifying field devices, central systems and staff composition. The complexity of the organization and the systems being managed play a prominent role in determining TMC Information Technology (IT) Security Guidelines.

The NIST Cybersecurity Framework and the CIS Top 20 Controls ultimately are comprised of recommendations for controlling hardware with access to the network, controlling software used on the devices on the network, controlling connectivity to the network, implementing controls and policies for staff with access to the network, systems and software, and ensuring resiliency, data protection and recovery.

This chapter will set a baseline for typical TMC composition as it relates to TMC IT security. Beyond Knowing/Identifying the TMC Critical Elements, other aspects of the Cybersecurity Framework functions will be discussed in subsequent chapters.

TMCs vary in size, responsibility, and complexity. As a result, there is no one-size-fits-all approach to cybersecurity. To capture the differences among TMCs and to obtain a baseline for prevailing practice, a Cybersecurity Maturity Questionnaire was distributed to TMCs of diverse types and sizes across multiple States to identify similarities and differences among various agency IT models and settings. Seventeen (17) complete responses were received from the following agencies:

1. Missouri Department of Transportation (DOT).
2. Minnesota DOT.
3. City of Sevierville, Tennessee.
4. Delaware DOT.
5. New Jersey Turnpike.
6. New York State DOT—Region 10.
7. New York State DOT—Region 4.
8. City of Austin, Texas.
9. City of Dallas, Texas.
10. City of Houston, Texas.
11. North Carolina DOT.
12. Georgia DOT.

[2] NIST, "Risk Management Framework for Information Systems and Organizations," October 2018. Retrieved from: https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/archive/2017-09-28.

[3] Center for Internet Security (CIS), "CIS Controls Version 7.1," 2019. Retrieved from: https://www.cisecurity.org/controls/.

13. Tennessee DOT.
14. Michigan DOT.
15. Illinois Tollway.
16. Regional Transportation Commission of Southern Nevada.
17. Arlington County, Virginia.

Due to the sample size, the discussion and analysis of responses is not intended to be a statistically significant representation of cybersecurity practices. Rather, the results are intended to capture the diversity of TMC sizes and responsibilities around the United States, to reveal areas of commonality and difference, to suggest areas in which the industry is doing well, and to suggest opportunities for improvement. A summary of the ways in which TMCs are characterized and categorized is included in this chapter. Best practice recommendations for TMC IT cybersecurity as they relate to these elements are included in subsequent chapters.

SIZE AND STAFFING

For classification purposes, the questionnaire asked respondents to self-assign their agency into one of three size categories: small, medium, or large. Large TMCs were categorized as TMCs with more than 10 operators during peak hours who manage over 500 devices. Medium sized TMCs had between 5 and 10 peak-hour operators who managed between 100 and 500 devices, and small TMCs had less than 5 peak-hour operators who managed less than 100 devices. Of the respondent agencies, one (1) self-identified as small, seven (7) as medium, and nine (9) as large.

In addition to staff size, it is important to be aware of staff composition and the security impacts associated with various staff types. Of the agencies surveyed, approximately half did not have any IT staff dedicated to the TMC, some had shared IT between different agency departments, some were dedicated but part of a separate centralized department serving the entire agency, and some had dedicated staff within the department. Furthermore, approximately half of the agencies surveyed reported that their IT was centrally managed, with the remaining half being managed by contractors or a combination of central staff and contract staff. No direct correlations were apparent between the staff mix versus the size or complexity of the TMC environment.

RESPONSIBILITIES

A TMC may be responsible for managing freeway operations, arterial highway operations, heavy rail operations, transit operations, or a combination of these. A TMC's focus may be urban or rural, regional or statewide. It may be single or multi-jurisdictional. TMC staff also may partner with other agencies to cover these variety of transportation networks, including police and transit.

TMCs employ any combination of the responsibilities below:

- Tolling (Revenue) Management.
- 511 Data or Video Management.
- Camera Monitoring.

- Dynamic Message Signs (DMS), Lane Control Signs (LCS), and Variable Speed Limit Signs (VSL) Content Management—permanent and portable.
- Ramp Metering.
- Traffic Signals Control.
- Microwave/Bluetooth/Wifi Readers Data Management.
- Connected Vehicle-to-Infrastructure (V2I) Equipment/Data Management.
- Environmental and/or Flood Sensor Management.
- Weigh-in-motion Management and Enforcement.
- Automatic Vehicle Location (AVL) System Management for Fleet Vehicles.
- Rail Notification System Management.
- Overheight Vehicle, Wrong Way, Truck Rollover, and Vehicle Speed Detection and Notification System Management.
- School Zone and Pedestrian Beacons and Information System Management.
- Highway Advisory Radio (HAR) Information System Management.
- Communications (cellular, hard-wire, wireless) Management.

DEVICE AND NETWORK MANAGEMENT

TMCs utilize a range of devices and equipment to collect data, disseminate information, and control operations. These devices require initial programming, ongoing maintenance and software updates, and in most cases, some means of data exchange with each other and/or the TMC. To that end, a variety of communications methods are common in the industry. A graphical depiction of these relationships developed by the United States Department of Transportation (USDOT) is shown in the figure on the following page.

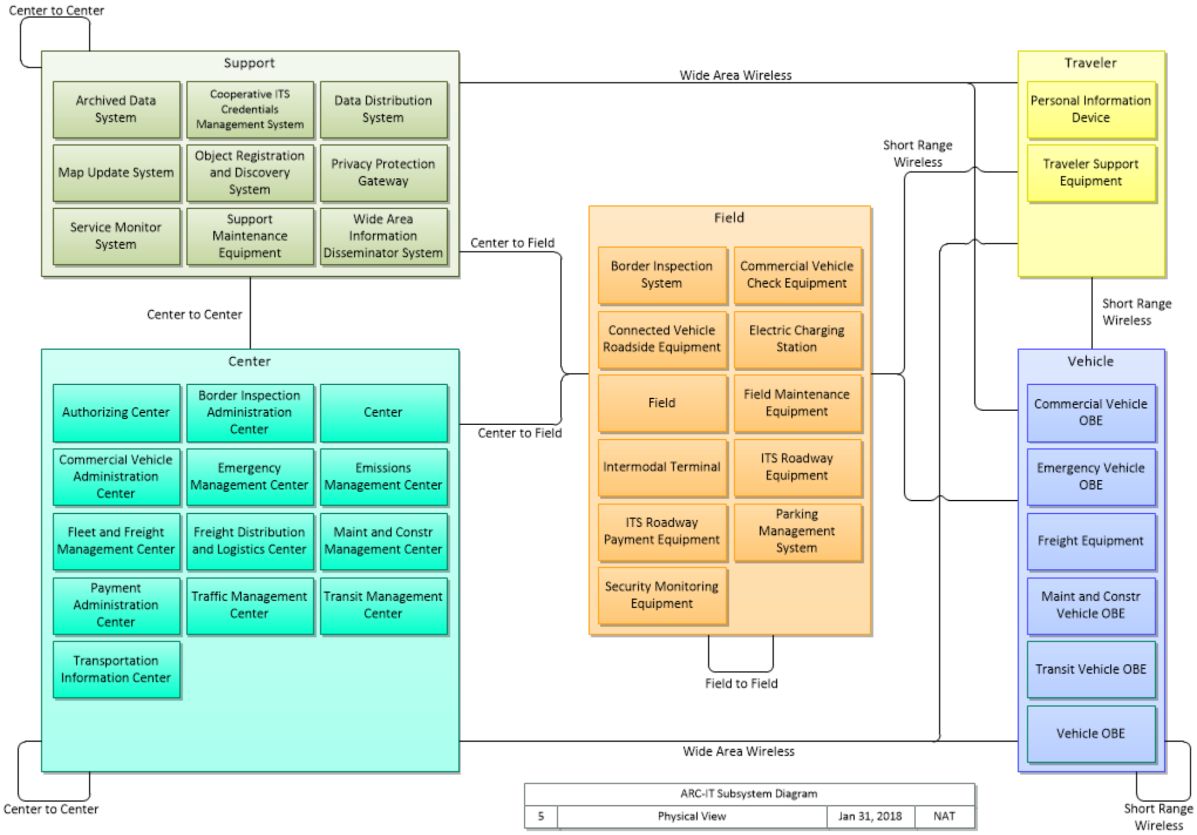

Center to Center
Support
Archived Data System
Cooperative ITS Credentials Management System
Data Distribution System
Map Update System
Object Registration and Discovery System
Privacy Protection Gateway
Service Monitor System
Support Maintenance Equipment
Wide Area Information Disseminator System
Wide Area Wireless
Traveler
Personal Information Device
Traveler Support Equipment
Short Range Wireless
Center to Field
Field
Border Inspection System
Commercial Vehicle Check Equipment
Connected Vehicle Roadside Equipment
Electric Charging Station
Field
Field Maintenance Equipment
Intermodal Terminal
ITS Roadway Equipment
ITS Roadway Payment Equipment
Parking Management System
Security Monitoring Equipment
Field to Field
Center to Center
Center
Authorizing Center
Border Inspection Administration Center
Center
Commercial Vehicle Administration Center
Emergency Management Center
Emissions Management Center
Fleet and Freight Management Center
Freight Distribution and Logistics Center
Maint and Constr Management Center
Payment Administration Center
Traffic Management Center
Transit Management Center
Transportation Information Center
Center to Field
Short Range Wireless
Vehicle
Commercial Vehicle OBE
Emergency Vehicle OBE
Freight Equipment
Maint and Constr Vehicle OBE
Transit Vehicle OBE
Vehicle OBE
Wide Area Wireless
Center to Center
ARC-IT Subsystem Diagram
5
Physical View
Jan 31, 2018
NAT
Short Range Wireless

Figure 3. Flowchart. National Intelligent Transportation System architecture physical view. (Source: National Intelligent Transportation Systems (ITS) Architecture.)

In the figure above, “wide area wireless” and “short range wireless” are two of the many communications types that may be utilized by a TMC for Center-to-Center, Center-to-Field, and Field-to-Field communications. Communications types commonly utilized by TMCs across the United States include twisted pair copper cable, fiber optic cable, licensed and unlicensed point to point or point to multi-point wireless, leased wired (i.e., broadband), and leased wireless (i.e., cellular) communications. Each of these types of communications provides its own security concerns, many of which will be discussed at a high level in future chapters.

It also should be noted that some of these devices have limitations in the way they operate that make protection at the device difficult. For example, a wireless point to point radio transmitter is not housed in a locked enclosure and is exposed to potential tampering. In other cases, devices may be housed in a locked enclosure, but a series of standard physical keys may be shared across multiple agencies to access those enclosures. In most cases, devices or device groups access the communications network back to the TMC via network switches. It is important that these network switches/access points have security measures and encryption in place to control access to the system.

To protect the overall system further, some TMCs have deployed firewalls and other controls to protect network boundaries and create network separation. This is especially important between the field environment and the TMC environment. Some TMCs have multiple servers and/or off-site data storage or backup to provide an additional layer of separation and redundancy.

CHAPTER 3. BEST PRACTICES FOR TRAFFIC MANAGEMENT CENTERS INFORMATION TECHNOLOGY SECURITY

BEST PRACTICES DISCUSSION

While synthesizing the available resources on Information Technology (IT) cybersecurity, sources from the Department of Homeland Security (DHS), the Center for Internet Security (CIS), and the National Institute of Standards and Technology (NIST) were considered for their relevance to Traffic Management Centers (TMC). Several agencies acknowledged and referenced the use of the NIST Cybersecurity Framework, while others used other agency directives to guide their control strategies. As a result of evaluating these different standards, some common themes were identified, including:

- Risk-management approaches should be applied to control center cybersecurity.

- Network segmentation should be maintained between "business" infrastructure (i.e., payroll/accounting systems, human resources, email, and other systems used to manage the business environment of the agency) and industrial control infrastructure. While there are different ways to achieve segmentation using logical (e.g., Virtual Local Access Networks (VLAN)) and physical separation (e.g., firewalled or even air-gapped), it should be noted that logical is not as secure as physical separation.

- Established partnerships with other TMCs, transportation departments and Federal support organizations can serve as a critical support network.

- The deployment of Internet-connected technologies and standard communication protocols within industrial control environments is increasing risk exposure for TMCs.

- The need for increased collaboration between IT and Operations Technology (OT) staff.

From the analysis, it was determined that the NIST Cybersecurity and Risk Management Frameworks were more abstract and strategic in nature, while the CIS Top 20 Controls provide more technical detailed guidelines of immediate benefit to TMC operators. Thus, using the CIS Top 20 Controls in baselining security measures provides an immediate impact on guiding control of hardware, software and networks in the TMC, while the NIST frameworks can play a beneficial role to supplement with strategic visioning of Risk Management Plans and Resiliency Plans. The purpose of this report is not to replicate the guidelines in these frameworks, but rather to highlight the guidelines most relevant to TMC IT cybersecurity.

Risk management begins with the awareness of what vulnerabilities the TMC is exposed to, based on the characteristics of the staffing (employees and contract staff), the types of devices and how they are connected to the network, and the software used throughout to control and management operations. Cybersecurity self-assessments for the organization also are discussed as a prioritization strategy in chapter 5.

Implementing *CIS Top 20* building blocks for Internet security provides a layered approach to addressing all areas of risk exposure. The CIS Controls are separated into Basic, Foundational, and Organizational levels of IT security management. A complete list of the controls for IT security is provided in figure 4 below. Controls that can be applied to TMC IT/OT security will be discussed in further detail in subsequent chapters.

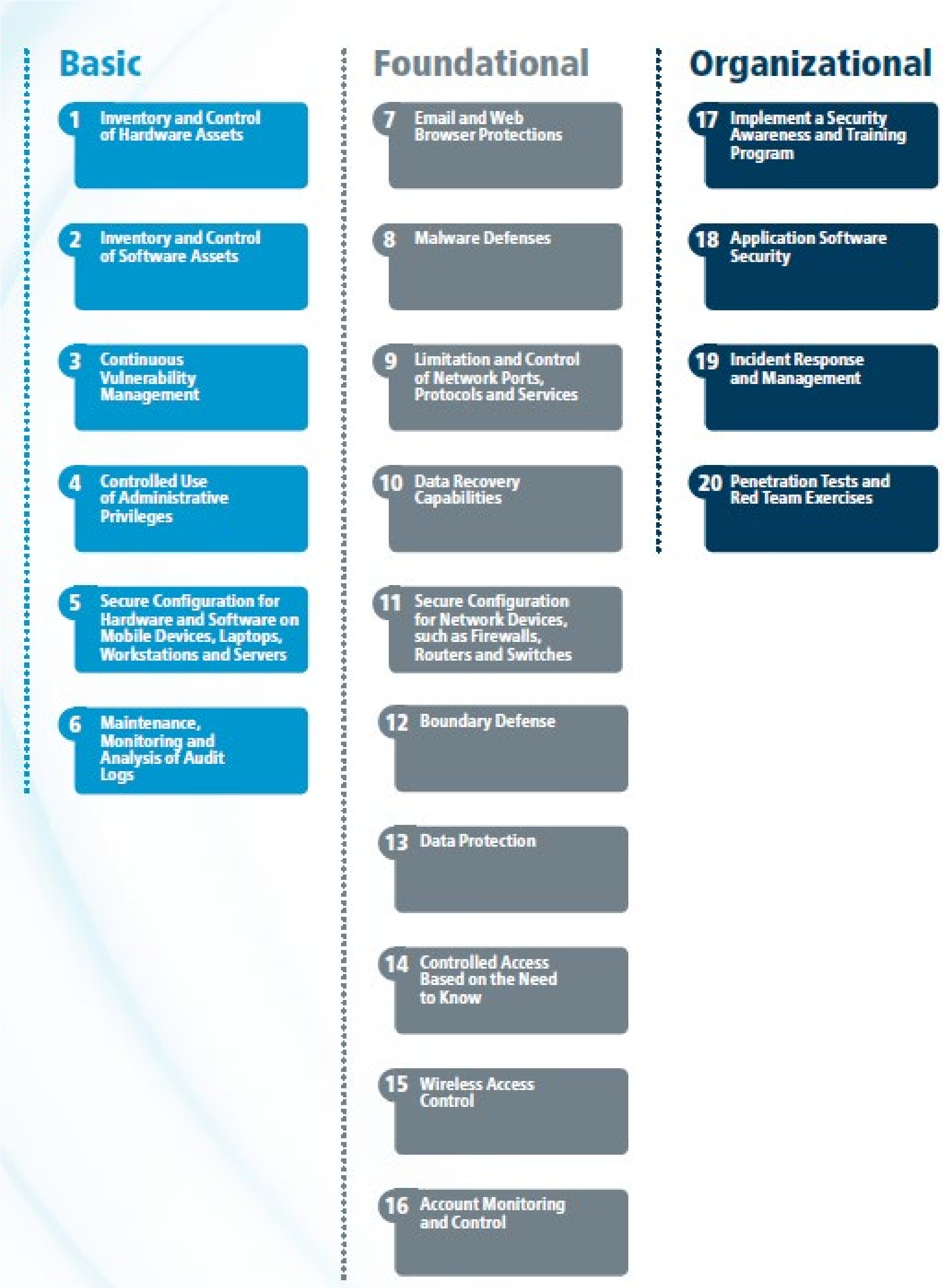

Basic
1 Inventory and Control of Hardware Assets
2 Inventory and Control of Software Assets
3 Continuous Vulnerability Management
4 Controlled Use of Administrative Privileges
5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6 Maintenance, Monitoring and Analysis of Audit Logs
Foundational
7 Email and Web Browser Protections
8 Malware Defenses
9 Limitation and Control of Network Ports, Protocols and Services
10 Data Recovery Capabilities
11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
12 Boundary Defense
13 Data Protection
14 Controlled Access Based on the Need to Know
15 Wireless Access Control
16 Account Monitoring and Control
Organizational
17 Implement a Security Awareness and Training Program
18 Application Software Security
19 Incident Response and Management
20 Penetration Tests and Red Team Exercises

Figure 4. Chart. Center for Internet Security top 20 critical security controls version 7.1. (Source: CIS Controls Version 7.1.)

The National Institute of Standards and Technology Risk Management Framework

As a primer to establishing the TMC IT Security guidelines in this report, it is worth a quick review of the NIST Risk Management Framework for conducting cybersecurity risk management. This framework provides a set of six (6) steps for managing risk, which are shown within the inner-circle of the figure below. The figure from NIST SP 800-37 illustrates the risk management process in context with other Federal Information Processing Standards (FIPS) and other Special Publication (SP) references.[4]

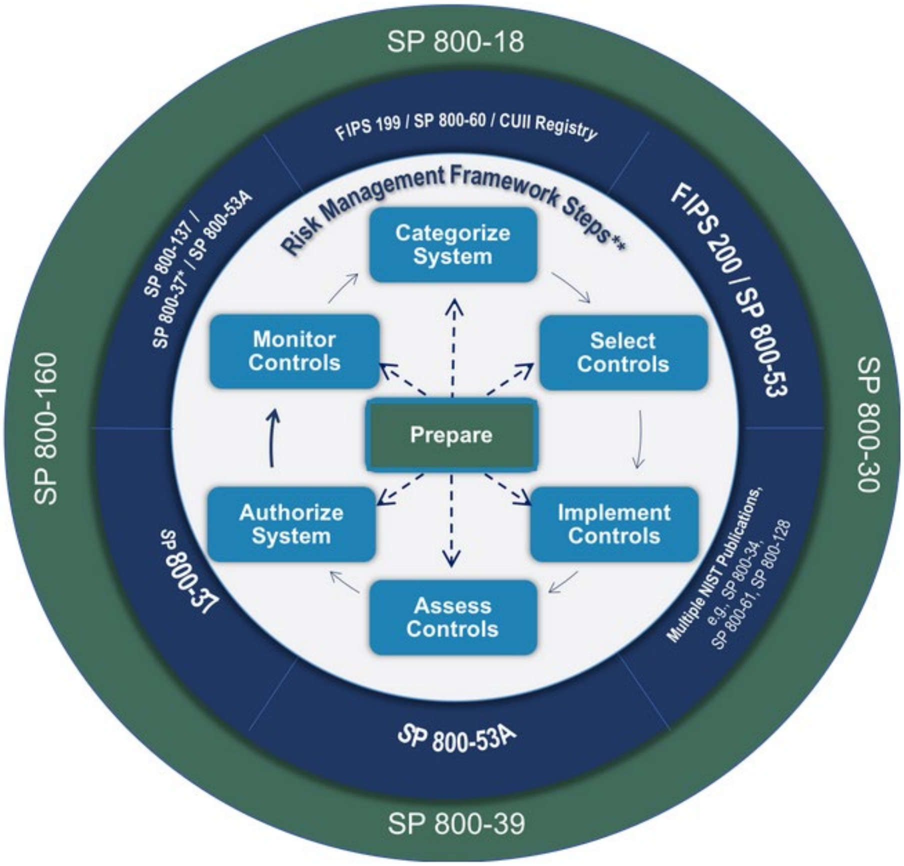


Figure 5. Flowchart. The National Institute of Standards and Technology risk management framework.
(Source: NIST SP 800-37 Risk Management Framework.)

As this is the most well documented risk management methodology proposed by the Federal Government, it is directly applicable to any TMCs that choose to pursue a risk management-based cybersecurity strategy.

Some agencies, particularly those with connections to the Federal sector also will need to stay apprised of NIST 800-53 (for Federal information systems/organizations) and FedRAMP (for

[4] NIST, "SP 800-37 Rev. 2 Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach," 2018. Retrieved from: https://csrc.nist.gov/publications/detail/sp/800-37/rev-1/final.

cloud hosting).[5] While this document focuses on broader guidelines for TMCs, some organizations may find the NIST documentation helpful in evaluating, selecting and specifying information systems or controls for subsystems within the TMC environment. Two relevant NIST documents will be useful for supplementing CIS Top 20 for chapters 8 and 9 for administrative policies and resiliency plan development:

- NIST 800-53 Security and Privacy Controls for Federal Information Systems and Organizations.
- NIST 800-82 Guide to Industrial Control Systems (ICS) Security.[6]

Additionally, while most TMCs do not process billing information for credit cards associated with tolling or fare collection systems, it should be noted that agencies having this responsibility also are obligated to comply with Payment Card Industry Data Security Standards (PCI-DSS) for processing back-office toll payments and other credit card financial transactions. The goals of PCI-DSS are compatible with NIST Cybersecurity Framework and CIS Top 20, and are built to maintain a secure network, protect cardholder data, maintain a vulnerability management program, implement strong access control measures, regularly monitor and test networks, and maintain an information security policy.

Best Practices Scan of Traffic Management Center Operators

This section will summarize noteworthy practices identified by agencies responding to the questionnaire and existing reference literature and correlating them to the CIS Top 20 controls. During a scan of several TMC operators across the country of varying sizes, the following cybersecurity practices currently are being employed by one or more organizations:

1. **Using active and/or passive scanning tools to identify all devices attached to the network on a routine basis** (relevant to CIS Control 1). Manually documenting devices on the network can quickly become outdated. Using industry available tools to expedite the initial process, as well as allowing for continued monitoring and updates is worthwhile in a dynamic environment such as TMCs.

2. **Vendor-supported software residing on a demilitarized zone (DMZ) section of the network**, so that remote support by Secure Sockets Layer (SSL) Virtual Private Network (VPN) access is only granted to the DMZ and not to the enterprise/business network (relevant to CIS Control 2). Some applications often require communications with field devices and other subsystems, but generally do not require direct access to the enterprise environment. Restricting access by remote vendors limits risk exposure and the potential attack surface on the most critical infrastructure/systems.

[5] NIST, “SP 800-53 Rev. 4 Security and Privacy Controls for Federal Information Systems and Organizations,” 2015. Retrieved from: https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final.

[6] NIST, “SP 800-82 Rev. 2 Guide to Industrial Control Systems (ICS) Security,” 2015. Retrieved from: https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final.

3. **Using Access Control Lists (ACL) or equivalent network access techniques** to limit outside access to specific machines or services, so that access is granted only to the devices/networks that need them (relevant to CIS Control 14), or essentially managing the users/devices with a "need to know." This also is a relevant method for managing insider vulnerabilities, particularly for limiting the range of systems available through remote access configurations.

4. **Requiring background checks for personnel that require access to control rooms**, particularly with direct administrative/privileged access to software, systems, and data centers (relevant to CIS Control 14). When coupled with enforcing detailed logging of changes to configurations and data, this practice provides a solid basis for data protection and assistance for managing insider vulnerabilities (relevant to CIS Control 13).

5. **Leveraging existing security policies governing the entire agency, not just the TMC**. In the past, many TMCs operated as an island from all other enterprise network platforms. However, today it is critical to be interconnected with the multitude of data systems internal and external to an agency. Some larger TMCs are nearly self-autonomous from a policy-making standpoint, but a number of those surveyed indicated some level of existing IT policy governing the entire agency, not just the TMC. This is an organizational arrangement that broadly relates to CIS Controls 17 through 20. TMCs may be independently in control of their respective subsystems but should recognize the importance of embracing/incorporating existing policy frameworks for the broader organization while addressing the gaps that are specific/unique to the TMC environment.

6. **Updating cybersecurity policies at least once a year to fix anomalies in the procedures based on current trends** (relevant to CIS Control 17 and 19). Policies should be evaluated annually or when an incident occurs and should be reviewed against updates to NIST guidelines and relevant policies that the agency is using. During these timeframes, agencies also should assess their achievements with respect to all CIS Controls identified in their respective Risk Management Plan.

GAPS/AREAS OF IMPROVEMENT

More so than trends, the review of several TMC operators during the survey process gave indication of notable areas in need of improvement within the industry. The following areas of concern have been identified, along with the importance of each, though they are not necessarily widespread issues for all organizations:

1. **Network port security solutions, and the use of certificates to authenticate devices is not widely adopted** (relevant to CIS Control 1).

2. **There does not appear to be widespread adoption of software/application whitelisting among TMC operators** (relevant to CIS Control 2). This is a technique used to only allow software applications that are acknowledged/approved to be run on the network.

3. **The majority of TMC organizations have not performed a skills gap analysis to understanding the skills and behaviors of their workforce** (relevant to CIS Control 17).

4. **The importance of patch management is not widely acknowledged** (relevant to CIS Control 3).

5. **Multi-factor authentication is still lacking across many TMC systems** (relevant to CIS Control 4 and 16). Weak password practices are a key factor in unauthorized user access, much of which can be mitigated through secondary authentication methods.

6. **TMCs need to implement routine incident response exercises** (relevant to CIS Control 19). Without going through an example breach, it is difficult to appreciate what will happen when one is encountered, and whether the existing policies are there to address it.

7. **There is an identified shortage of dedicated versus consolidated IT staff for TMCs** (relevant to CIS Control 17). Partnering with the broader organization to resolve hiring and/or training needs is a critical piece to overcoming this gap. Partnering between OT and IT should be encouraged to increase awareness of the challenges that both ends face with respect to balancing security with ease of operational functionality.

THE ROLE OF CONSTRUCTION/PROCUREMENT METHODS IN TRAFFIC MANAGEMENT CENTER INFORMATION TECHNOLOGY SECURITY

Transportation agencies are subject to public procurement guidelines and are accustomed to designing projects and putting them out to bid. However, the TMC environment and the IT portion of that environment have increasingly become classified as sensitive or critical infrastructure information to be guarded from the public domain. Agencies should have policies and guidelines in place for determining what aspects of their construction plans qualify as sensitive information and manage the procurement accordingly. For instance, some agencies establish on-call contracts with vetted contractors that also have executed non-disclosure agreements, and only issue work orders for upgrades to the network or the facility to prevent sensitive information entering the public domain. Others will issue a two-step Invitation for Bid (IFB) to pre-qualify potential contractors before releasing copies of the plans to them. These are examples of the use of procurement methods to mitigate the risks associated with exposing a TMC's critical infrastructure information in the public domain.

Relegating the configuration settings for network devices to installation contractors also should be verified to ensure adherence to TMC network configuration policies identified with CIS Controls. When possible, TMC IT staff should provide configuration files and prevent alterations of those configurations instead of leaving it to the contractors to maintain control of the hardware, software, and network assets in the TMC.

Supply chain attacks against hardware and software vendors are becoming more common. Procurement through reputable sources are a minimum best practice but establishing prenegotiated periods for responding to security issues with upgrades/patches is an important consideration for procurement of software and hardware contracts, particularly for specialized equipment related to ICS vendors. Additionally, this and other examples of cybersecurity procurement language for control systems has been provided for various subsystems by U.S. Computer Emergency Response Teams (US CERT).[7] Many medium-to-large TMCs use a dedicated/isolated test environment to validate upgrades and patches before loading into the production environment to minimize risks from supply chain.

[7] Department of Homeland Security (DHS), "Cyber Security Procurement Language for Control Systems," 2009. Retrieved from: https://ics-cert.us-cert.gov/sites/default/files/documents/Procurement_Language_Rev4_100809_S508C.pdf.

CHAPTER 4. TECHNICAL GUIDELINES AND RECOMMENDED PRACTICES

This section provides the introduction to the technical guidelines and recommended practices in chapters 5 through 9, which build a culture of Operations Technology (OT)/Information Technology (IT) security for Traffic Management Centers (TMC); keeping it at the process/organizational structure level and related to the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) and Center for Internet Security (CIS) Top 20 Controls.

The NIST Cybersecurity Framework provides guidelines for how organizations can assess and improve the ability to secure their environments, manage risk, and respond to threats. The five areas for NIST Cybersecurity Framework core functions are as follows:

- **Know (Identify):** Activities to identify what systems need to be protected, assess priority considering organizational mission, and manage processes to achieve cost-effective risk management goals.

- **Protect:** Categories of management, technical, and operational activities that enable the organization to decide on the appropriate outcome-based actions to ensure adequate protection against threats to business systems that support critical infrastructure components.

- **Detect:** Activities that identify (through ongoing monitoring or other means of observation) the presence of undesirable cyber risk events, and the processes to assess the potential impact of those events.

- **Respond:** Specific risk management decisions and activities enacted based upon previously implemented planning (from the Protect function) relative to estimated impact.

- **Recover:** Categories of management, technical, and operational activities that restore services that have previously been impaired through an undesirable cybersecurity risk event.

The CIS Top 20 were developed to provide organizations with a smaller, prioritized number of actionable controls that should be implemented first. The CIS Top 20 outline Critical Security Controls (CSC) that organizations can use to establish a baseline for protection of their environment.

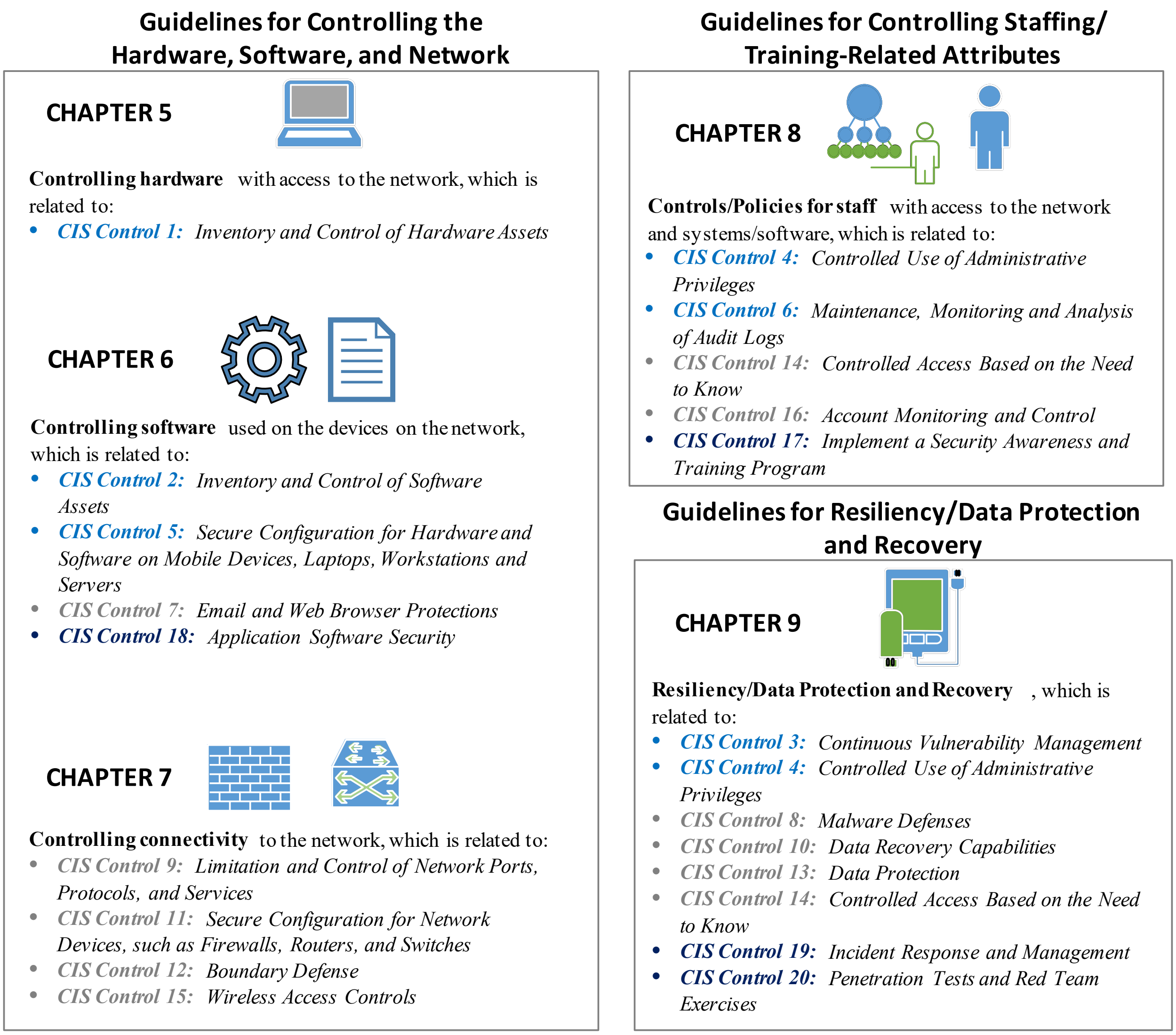
A TMC environment, along with supporting staff, is typically comprised of individuals with distinct roles focused on managing three areas:

- Information technology/systems (subdivided to address networking, devices, hardware, and software).
- Personnel (i.e., human resources).

- Administrative and contractual data management practices (e.g., Freedom of Information Act (FOIA) requests, data archival and organizational resiliency, etc.).

The CIS Top 20 Critical Security Controls correspond to these three functional areas, and each CIS sub-control is relevant to one of the three TMC roles.

The first TMC role, which is subdivided to address hardware, software, and networking within the overall information technology management area, will be covered in chapters 5, 6, and 7, respectively. Chapter 8 highlights guidelines relevant to personnel controls and elements associated with insider vulnerabilities. Chapter 9 covers controls associated with data protection and resiliency. The figure below shows the CIS controls that are relevant to each of these TMC roles. They have been color-coded to match the ***Basic***, ***Foundational***, and ***Organizational*** control labeling in the CIS document figures shown in chapter 3.



Guidelines for Controlling the Hardware, Software, and Network

CHAPTER 5

Controlling hardware with access to the network, which is related to:

- *CIS Control 1: Inventory and Control of Hardware Assets*

CHAPTER 6

Controlling software used on the devices on the network, which is related to:

- *CIS Control 2: Inventory and Control of Software Assets*
- *CIS Control 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers*
- *CIS Control 7: Email and Web Browser Protections*
- *CIS Control 18: Application Software Security*

CHAPTER 7

Controlling connectivity to the network, which is related to:

- *CIS Control 9: Limitation and Control of Network Ports, Protocols, and Services*
- *CIS Control 11: Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches*
- *CIS Control 12: Boundary Defense*
- *CIS Control 15: Wireless Access Controls*

Guidelines for Controlling Staffing/ Training-Related Attributes

CHAPTER 8

Controls/Policies for staff with access to the network and systems/software, which is related to:

- *CIS Control 4: Controlled Use of Administrative Privileges*
- *CIS Control 6: Maintenance, Monitoring and Analysis of Audit Logs*
- *CIS Control 14: Controlled Access Based on the Need to Know*
- *CIS Control 16: Account Monitoring and Control*
- *CIS Control 17: Implement a Security Awareness and Training Program*

Guidelines for Resiliency/Data Protection and Recovery

CHAPTER 9

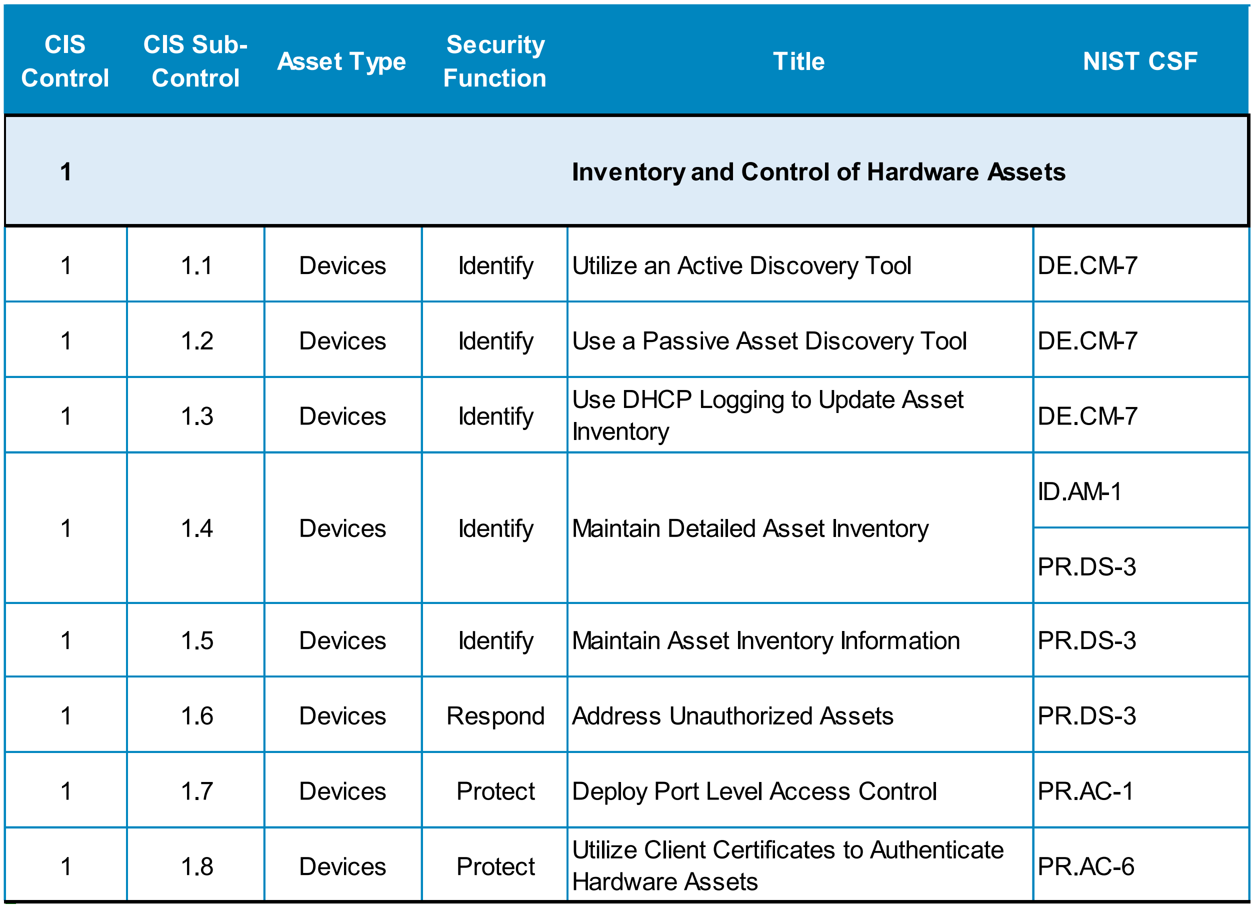
Resiliency/Data Protection and Recovery , which is related to:

- *CIS Control 3: Continuous Vulnerability Management*
- *CIS Control 4: Controlled Use of Administrative Privileges*
- *CIS Control 8: Malware Defenses*
- *CIS Control 10: Data Recovery Capabilities*
- *CIS Control 13: Data Protection*
- *CIS Control 14: Controlled Access Based on the Need to Know*
- *CIS Control 19: Incident Response and Management*
- *CIS Control 20: Penetration Tests and Red Team Exercises*

Figure 6. Chart. Relationship between Center for Internet Security Controls and Traffic Management Center roles.(Source: Federal Highway Administration.)

While the predominant focus of these guidelines is on the CIS Controls, mapping between CIS and NIST has been developed by CIS and can be used by organizations focusing in one set of controls or the other.[8]

In the appendices, a full copy of the CIS to NIST mapping is printed based on the current date of this report. However, users of these guidelines are encouraged to go to the CIS Controls website for the most current version. A subset of CIS Control 1 is provided below as a reference for the associated cross-mapping. A summary table of the controls associated with each topic area in chapters 5 through 9 has been provided at the end of each topic, focusing on the relevant CIS controls. Agencies that already are involved with the use of NIST are advised to reference the appendices for the complete list of associated NIST CSF activities associated with the recommended CIS Controls documented herein.



CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	NIST CSF
1				**Inventory and Control of Hardware Assets**	
1	1.1	Devices	Identify	Utilize an Active Discovery Tool	DE.CM-7
1	1.2	Devices	Identify	Use a Passive Asset Discovery Tool	DE.CM-7
1	1.3	Devices	Identify	Use DHCP Logging to Update Asset Inventory	DE.CM-7
1	1.4	Devices	Identify	Maintain Detailed Asset Inventory	ID.AM-1 PR.DS-3
1	1.5	Devices	Identify	Maintain Asset Inventory Information	PR.DS-3
1	1.6	Devices	Respond	Address Unauthorized Assets	PR.DS-3
1	1.7	Devices	Protect	Deploy Port Level Access Control	PR.AC-1
1	1.8	Devices	Protect	Utilize Client Certificates to Authenticate Hardware Assets	PR.AC-6

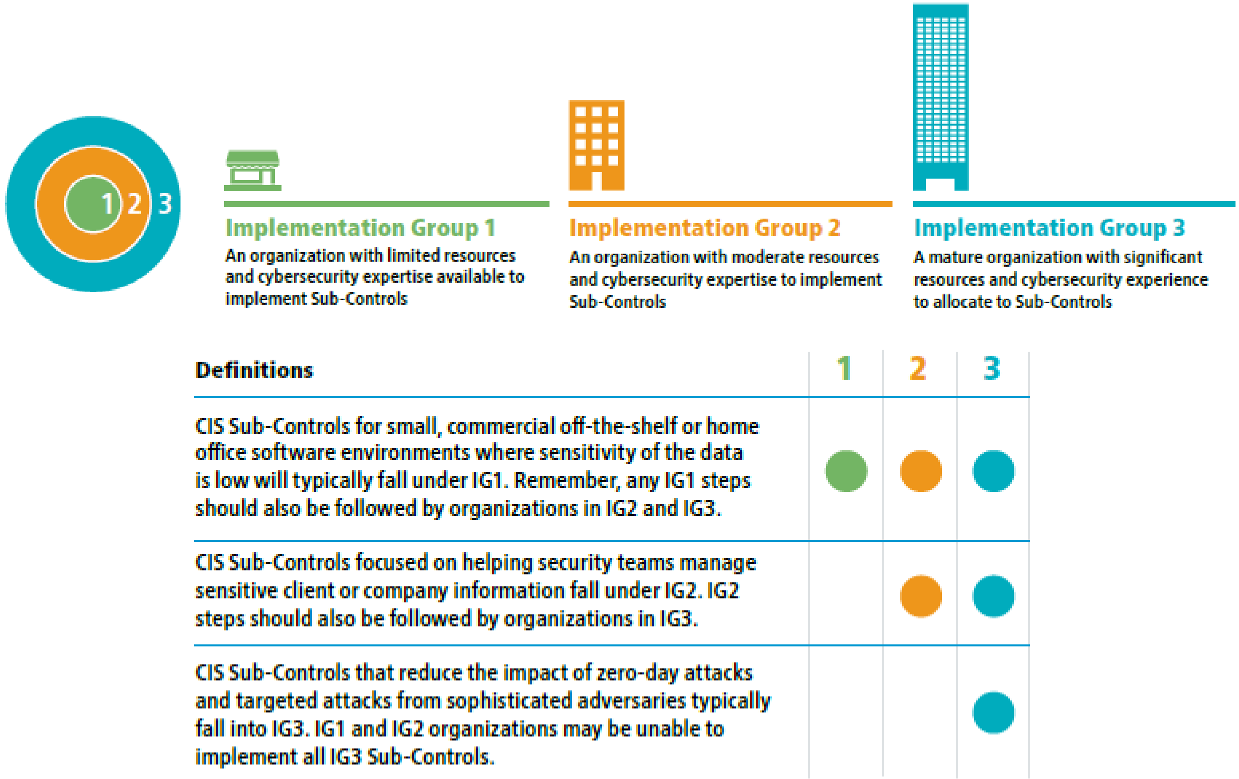
Figure 7. Screenshot. Center for Internet Security controls mapping to the National Institute of Standards and Technology security functions and the National Institute of Standards and Technology cybersecurity framework. (Source: CIS Controls Version 7.1.)

[8] Center for Internet Security (CIS), "CIS Controls V7.1 Mapping to NIST CSF." Retrieved from: https://www.cisecurity.org/white-papers/cis-controls-v7-1-mapping-to-nist-csf/.

Additionally, DHS has developed a similar mapping document to map NIST controls to Cyber Resilience Review (CRR) controls.[9] The emphasis on CIS Controls provides a central approach that can be used throughout these guidelines, and readily accommodates cross-referencing between the other frameworks for additional supporting information.

While it will not eliminate all risks, using the following guidelines can provide ways to manage and control those risks. Relevant CIS Top 20 Controls are incorporated into each subsection as noted above.

CIS Controls version 7.1 has been structured in layers based on an organization's size and sophistication. The following diagrams from v7.1 shows three levels of organizational capabilities.



Implementation Group 1
An organization with limited resources and cybersecurity expertise available to implement Sub-Controls

Implementation Group 2
An organization with moderate resources and cybersecurity expertise to implement Sub-Controls

Implementation Group 3
A mature organization with significant resources and cybersecurity experience to allocate to Sub-Controls

Definitions	1	2	3
CIS Sub-Controls for small, commercial off-the-shelf or home office software environments where sensitivity of the data is low will typically fall under IG1. Remember, any IG1 steps should also be followed by organizations in IG2 and IG3.	●	●	●
CIS Sub-Controls focused on helping security teams manage sensitive client or company information fall under IG2. IG2 steps should also be followed by organizations in IG3.		●	●
CIS Sub-Controls that reduce the impact of zero-day attacks and targeted attacks from sophisticated adversaries typically fall into IG3. IG1 and IG2 organizations may be unable to implement all IG3 Sub-Controls.			●

Figure 8. Infographic. Center for Internet Security implementation groups. (Source: CIS Controls version 7.1.)

Within the CIS Controls document, as the organization reviews recommendations for protecting the TMC, priority should be given to those that are recommended for all three implementation groups, followed by those recommended for groups 2 and 3, and finally those applicable to just group 3. It is anticipated that the majority of TMCs will fall into group 2. Some smaller

[9] Department of Homeland Security (DHS), "Cyber Resilience Review (CRR): NIST Cybersecurity Framework Crosswalks," 2016. Retrieved from: https://www.us-cert.gov/sites/default/files/c3vp/csc-crr-nist-framework-crosswalk.pdf.

organizations will fall into group 1. Larger organizations, or those abiding within regulatory scrutiny, will fall into group 3.

For TMCs, since the primary recommendation is to follow CIS Controls for initial guidelines, this section will focus heavily on each of those CIS Top 20 Controls. Within each CIS Control, the sub-controls focus on a type of asset (e.g., Users, Networks, Applications, Devices, and Data), and the security function (e.g., *Identify*, *Protect*, *Detect*, *Respond*), which correlate to NIST Cybersecurity Framework elements.

CHAPTER 5. GUIDELINES FOR CONTROLLING HARDWARE WITH ACCESS TO THE NETWORK

To determine if something is out of the ordinary, it is necessary to know/identify what "ordinary" is. That is the premise of ***Center for Internet Security (CIS) Control #1:*** *Inventory and Control of Hardware Assets*. Whether an organization decides to use an active or a passive discovery tool to start or maintain tracking the network-attached devices, maintaining a detailed asset inventory is at the top of the list for Control #1. Without knowing what devices are supposed to be on the network, it is difficult to maintain control of the network.

A detailed inventory of devices connected to the network begins with *identifying* each device's location, respective IP address, Media Access Control (MAC) address, and manufacturer name. At a minimum, this should consist of anything connected to the Traffic Management Center (TMC) network in the building: servers, workstations, wireless access points, video wall controllers, network video recorders, security/surveillance systems, access control systems, firewalls, switches, routers, printers, copiers, wireless thermostats, any other network appliances or devices.

After identifying the elements of the TMC network environment, the next step is to implement device controls to *protect* the network and related systems. Port-level access controls (i.e., port management), like IEEE 802.1x and network access control (NAC), are highly recommended for the enforcement of device access policies and to prevent unauthorized devices from connecting to the network through open network ports on the TMC floor or Wireless local area network (LAN) access points.

For further control and protection, devices that do not support port-level access controls can be isolated by Virtual Local Access Network (VLAN), but firewalls are preferable for more critical systems. This also is true for printers, copiers, and other devices (including leased devices from service companies) that contain data storage devices. Mobile devices (phones, tablets, etc.) that are not controlled by an administrative operating system (i.e., bring-your-own-devices (BYOD) or computers with temporary guest access) or port controls noted above should be considered a risk with appropriate connection protection to the enterprise network (e.g., network authentication appliances, firewalls, multi-factor authentication, or equivalent) to prevent rogue devices from directly accessing the enterprise network. Given the wide range of vendors and network appliances in use within a TMC environment, another common best practice is to establish a test environment apart from the production environment. Network appliance vendors and field device vendors for Operations equipment routinely roll out software/firmware updates, which are best to test in the isolated Test environment before putting the Production environment at risk if the vendor's updates have been compromised.

> Given the wide range of vendors and network appliances in use within a TMC environment, another common best practice is to ***Establish a Test Environment*** apart from the production environment.

RELEVANT CONTROLS FOR HARDWARE/DEVICES

- *CIS Control 1: Inventory and Control of Hardware Assets.*

Some TMCs manage tunnels at water crossings or through mountains. As such, ventilation systems, fire suppression systems, flood gates, and/or other Supervisory Control and Data Acquisition (SCADA)-type systems are more likely to be encountered in these environments. For TMCs with SCADA industrial control system (ICS) exposure, limit access to Internet-based devices to the specific protocols/ports necessary, ensure that default username and passwords have been erased or replaced, and evaluate the applicability of National Institute of Standards and Technology (NIST) SP 800-82 for those ICS/SCADA components. Section 4.1.2 of NIST SP 800-82 recommends evaluating the risks on SCADA systems for their physical, economic, and/or social impacts to help the agency decide about isolating these systems from the rest of the network.

Going forward, continually monitor what devices are connected to the network, and quarantine and/or remove unauthorized assets in a timely manner. Larger organizations should employ active asset management tools (e.g., OpenNMS, SolarWinds, Nagios, PRTG, and other industry examples) to scan the network, add/monitor for new devices, and flag them before granting immediate access.

CHAPTER 6. GUIDELINES FOR CONTROLLING SOFTWARE USED WITHIN THE NETWORK

Traffic Management Centers have a wide range of software applications ranging from vendor-provided software that is specific to managing a single type of Intelligent Transportation Systems (ITS) field device/subsystem, to a custom-developed software platform that integrates all field devices into one system. These may reside on individual server hardware platforms or within one or more Virtual Machines (VM) on servers(s). Advanced adversaries are continuously conducting research and development to identify new vulnerabilities in the applications used by their targets and the infrastructure on which those applications run. Similar to hardware control, software control begins with an inventory to *identify* what is present on the Traffic Management Center (TMC) network. ***Center for Internet Security (CIS) Control 2:*** *Inventory and Control of Software Assets* provides guidelines on managing software deployed within the TMC and underscores the importance of the removal of unnecessary software, which poses a risk due to potential security flaws or lack of vendor support, as well as determining appropriate separation of high-risk applications from the most critical systems. As an example, if a traffic management software vendor ceases to support upgrades to use the newest Windows operating system, and Microsoft also stops supporting patches for the older operating system, both will be compromised from a security standpoint, which should be addressed before a problem arises. Additionally, TMCs with custom software tend to deploy a test environment and a live-production environment segmented on different parts of the network. In those cases, devices that are moved back and forth between the two networks and should be tracked and regularly checked for accuracy.

Once a baseline is established, maintaining control is equally important. Going forward, continually monitor what software applications are on each computer, and quarantine and/or remove unauthorized applications in a timely manner to maintain control. Quarantining an application may result in administrative rights being altered to restrict users from using the software until further evaluation and approval by TMC Information Technology (IT) staff.

Preventing unauthorized applications from being installed in the first place is a combination of ***CIS Control 2*** (e.g., whitelisting authorized applications) and ***CIS Control 5:*** *Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers* (e.g., maintain secure configuration settings for computer operating systems to minimize administrative privileges on what can be added/deleted/changed). These two CIS Controls are considered basic elements to all agencies that should be the starting point of security initiatives. The next two relevant CIS Controls are considered foundational and organizational, respectively. As such, they have more value once basic elements have been covered first. The next control element for software components is ***CIS Control 7:*** *Email and Web Browser Protections,* begins to address attack elements focused on end users' interactions with Internet-connected applications, which can expose the network and systems to malicious code and/or provide unauthorized access to the network by pilfering passwords through a variety of exploitation methods including social engineering. Two of the most relevant sub-controls of CIS Control 7 for all organizations involves ensuring that only fully supported browsers and email clients are allowed on the network, as well as using domain name system (DNS) filters to block access to known malicious domains. For example, if the agency is not doing business in a capacity that requires access to foreign country web domains, then restricting access to those domains can help prevent unnecessary exposure by reducing the attack surface on the network.

For larger organizations with a mixture of applications developed in-house along with vendor-supported applications, ***CIS Control 18:*** *Application Software Security* provides guidelines for procedural measures to be incorporated to routinely evaluate, monitor and correct exposure risks associated with application development and maintenance; because this is intended for more sophisticated TMC environments, the associated sub-controls are pertinent to group 2 and group 3 organizations. If the organization has sensitive applications or data sources that are passing across or outside the network, and it is desired to encrypt the entire data flow, the use of standardized encryption algorithms is highly recommended (sub-control 18.5).

CLOUD HOSTING

As a sub-variation of controlling software in the TMC environment, while cloud computing is increasingly being used for either data storage and/or hosting applications (e.g., Software as a Service (SaaS) or Platform as a Service (PaaS)), CIS Controls do not specifically discuss application hosting in this regard, though it is recommended to use caution regarding storing data in the cloud. When evaluating the option for a cloud computing solution, agencies need to consider the associated risks and challenges that the specific solution may encounter. The National Institute of Standards and Technology's (NIST) Cloud Computing Security Working Group (NCC-SWG) developed a Risk Management Framework (RMF) in a Cloud Ecosystem, which shows a 6-step process with the items specific to cloud-computing highlighted in blue. A wiki page is available online for further information regarding the NCC-SWG.[10]

RELEVANT CONTROLS FOR SOFTWARE

- *CIS Control 2: Inventory and Control of Software Assets NIST RMF Identify.*
- *CIS Control 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers.*
- *CIS Control 7: Email and Web Browser Protections.*
- *CIS Control 18: Application Software Security.*

Three primary cloud service models are the most prevalent:

1. Software as a Service (SaaS).
2. Platform as a Service (PaaS).
3. Infrastructure as a Service (IaaS).

In the first, the end-user agency only gets access to the software (e.g., webmail client, maintenance management software, etc.) without regard for the computing hardware required to run it in the cloud. SaaS typically offers limited capabilities for integration with other data,

[10] TWiki, "NIST Cloud Computing Collaboration Site." Retrieved from: https://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/CloudSecurity.

systems, and platforms, and tends to lead toward vendor lock-in, and little flexibility to customize the application for the TMC. Subscribing to travel-time and crowd-source data streams is a common use of SaaS for TMCs, where the agency is able to receive the data streams and store the data locally to mitigate vendor lock-in, integration, or the need for customizations.

For a PaaS environment, the agency begins to take a more active role in picking the hosting environment with control of the applications that are deployed but very little control of the underlying servers, processors, and storage equipment. For an IaaS, an agency gains more control of the operating system, the selection of the hardware, and limited control of the network that connects their selected applications and devices together. The TMC's traffic management software generally requires a great deal of customization to integrate legacy field devices, protocols, and TMC-specific elements (video walls, video distribution systems, access controls) and a wide array of telecommunication connection options, not to mention agencies that share data and controls with other public agencies. Picking a cloud service model is a balance between control/integration flexibility and how much the agency can maintain/administer safely and securely on their own.

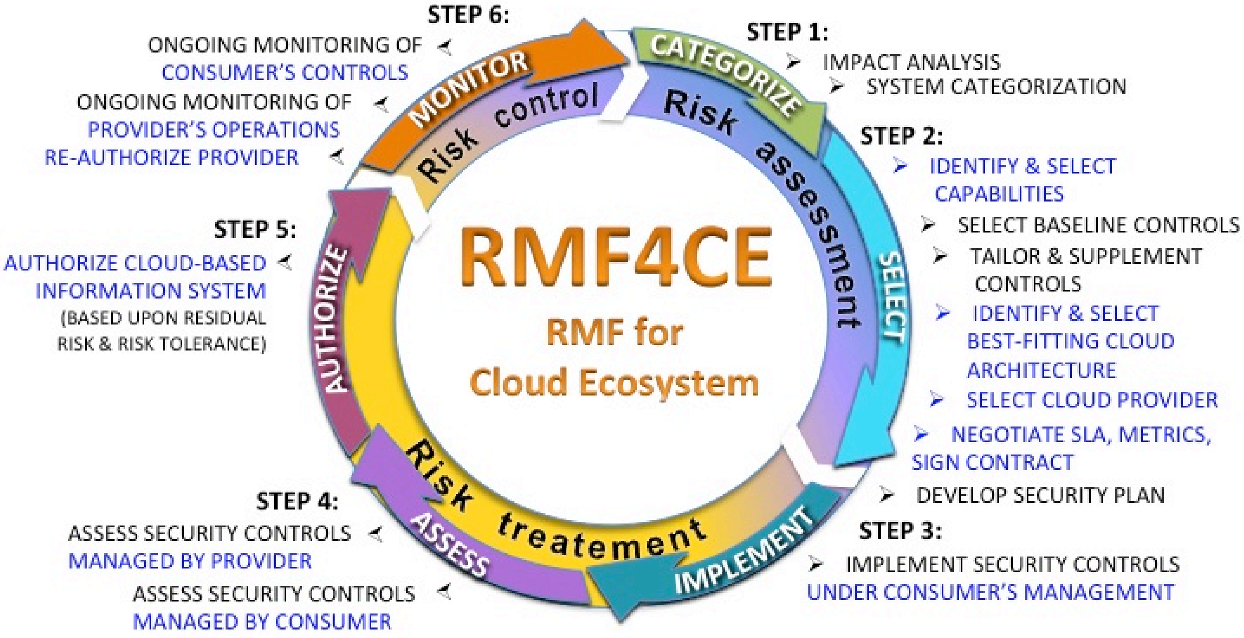

STEP 6:
ONGOING MONITORING OF CONSUMER'S CONTROLS
ONGOING MONITORING OF PROVIDER'S OPERATIONS
RE-AUTHORIZE PROVIDER
STEP 1:
IMPACT ANALYSIS
SYSTEM CATEGORIZATION
STEP 2:
IDENTIFY & SELECT CAPABILITIES
SELECT BASELINE CONTROLS
TAILOR & SUPPLEMENT CONTROLS
IDENTIFY & SELECT BEST-FITTING CLOUD ARCHITECTURE
SELECT CLOUD PROVIDER
NEGOTIATE SLA, METRICS, SIGN CONTRACT
DEVELOP SECURITY PLAN
STEP 3:
IMPLEMENT SECURITY CONTROLS UNDER CONSUMER'S MANAGEMENT
STEP 4:
ASSESS SECURITY CONTROLS MANAGED BY PROVIDER
ASSESS SECURITY CONTROLS MANAGED BY CONSUMER
STEP 5:
AUTHORIZE CLOUD-BASED INFORMATION SYSTEM
(BASED UPON RESIDUAL RISK & RISK TOLERANCE)
MONITOR
CATEGORIZE
SELECT
IMPLEMENT
ASSESS
AUTHORIZE
Risk control
Risk assessment
Risk treatement
RMF4CE
RMF for Cloud Ecosystem

Figure 9. Flowchart. Cloud consumers' view of the Risk Management Framework applied to a cloud ecosystem.
(Source: Managing Risk in a Cloud Ecosystem, NIST.)

Beyond choosing a cloud service model, there are several other elements that agencies need to consider when implementing a cloud-hosted environment. For instance, if the systems will be subject to the Federal guidance of FedRAMP due to the content being stored/shared, then the following guidelines need to be adopted by the organization:

- FedRAMP:
  - Per an Office of Management and Budget (OMB) memorandum dated December 8, 2011, any cloud services that hold Federal data must be FedRAMP authorized.[11] This memorandum also references NIST Special Publication 800-53 *Recommended Security Controls for Federal Information Systems and Organizations* and 800-53A regarding building effective security assessment plans.[12]
  - An agency official is responsible for making risk-based decisions to grant a cloud service provider with the Authority to Operate (ATO) along with the determined categorical NIST Federal Information Processing Standards (FIPS) 199 impact level of the applications/services.[13]
  - It also references NIST SP 800-144 *Guidelines on Security and Privacy in Public Cloud Computing.*[14] One key aspect involves maintaining accountability over the privacy and security of data and applications implemented in public cloud computing environments.
  - While these are the most applicable to TMCs, Federal agencies will need to abide by the broader list of referenced requirements to ensure compliance.
- Public cloud or GovCloud:
  - GovCloud platforms are operated by employees who are U.S. citizens on U.S. soil, and intended for hosting sensitive controlled unclassified information.
  - GovCloud U.S. regions are only accessible to U.S. entities, and these systems are restricted to root account holders who pass a screening process; agencies must confirm that they will only use a U.S. Person (green card holder or citizen as defined by the U.S. Department of State) to manage and access root account keys to the U.S. regions.

[11] Steven VanRoekel, Executive Office of the President "Security Authorization of Information Systems in Cloud Computing Environments Memorandum," 2011. Retrieved from: https://www.fedramp.gov/assets/resources/documents/FedRAMP_Policy_Memo.pdf.

[12] NIST, "SP 800-53A Rev. 4 Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans," 2014. Retrieved from: https://csrc.nist.gov/publications/detail/sp/800-53a/rev-4/final.

[13] NIST, "FIPS 199 Standards for Security Categorization of Federal Information and Information Systems," 2004. Retrieved from: https://csrc.nist.gov/publications/detail/fips/199/final.

[14] NIST, "SP 800-144 Guidelines on Security and Privacy in Public Cloud Computing," 2011. Retrieved from: https://csrc.nist.gov/publications/detail/sp/800-144/final.

- GovCloud is not an automatic requirement for TMCs looking to deploy systems in the cloud but is worth considering the value when an agency places more emphasis on trusting a third-party to maintain a key platform for them.

- Evaluate geographic diversity/availability for data storage in primary and secondary sites, and whether the organization can maintain control of where the data resides (in country or abroad for Public cloud providers).

- Evaluate the cloud providers support for protection against Internet attacks (e.g., Distributed Denial of Service (DDoS)) and other threats that the organization already protects against on the physical network.

- Evaluate cloud administrators access to the system data and whether an appropriate level of staff vetting is in place based on the level of access and/or risk.

CHAPTER 7. GUIDELINES FOR CONTROLLING NETWORK CONNECTIVITY

Tying back to the ability to prevent, alert, and respond to attacks on an agency's systems, this section of the report focuses on aspects pertaining to network connectivity and ways to manage connections with various subsystems (internally and externally) as well as recommendations for monitoring the network for unusual activity along with the ability to strategically respond in such a situation. The following are considered Foundational controls, as they build upon the basics identified above for establishing control of hardware and software components residing on the network. Once an organization has baselined its normal "ordinary" network, the next step is to strategically isolate critical infrastructure devices/systems, to limit risk exposure. ***Center for Internet Security (CIS) Control 9:*** *Limitation and Control of Network Ports, Protocols, and Services,* discusses separate ways in which agencies can limit and control access to certain devices and network segments. Devices that do not support these standards should be isolated to minimize risks of outside entities leveraging devices with weaker security features, which can be used to gain access to other parts of the network. Examples of ways to limit access are:

- Utilize ***port-filtering***[15] (sub-control 9.4) to manage the type of network traffic allowed on the network. Some vendors have even registered their preferred ports with the Internet Assigned Numbers Authority (IANA) such as Schneider Electric using port 5481, and GE using port 10212 for their respective Supervisory Control and Data Acquisition (SCADA) applications. The important consideration here is that when opening a port with access to the Internet, it is a recommended practice to limit the associated protocols that can use that port to prevent adversaries from using those ports as an attack vector. Also, this type of attack vector, and ways to circumvent it during an incident (e.g., configuring systems to use an alternate port number if possible), should be covered in an agency's risk management plan.

- Utilize a next-generation application firewall (sub-control 9.5) to provide application awareness, user identification, and content filtering. Allows administrators to define policy for users that are authorized to access specific applications and to ensure the content being passed is clear of exploits. While this is listed for implementation group 3, it is strongly recommended for group 2 as well since Traffic Management Centers (TMC) have a higher tendency to import/export data and applications with other entities.

- Client Certificates to authenticate computer assets connecting with the trusted network.

[15] In addition to an IP address for a device, the IANA manages the registration of commonly used port numbers used in conjunction to signify the kind of traffic that is being sent across the network. (Wiki, "List of TCP and UDP port numbers." Retrieved from: https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers.) Common examples include:

- Port 21 for File Transfer Protocol (FTP) traffic.
- Port 80 for hypertext transfer protocol (HTTP) web traffic.
- Port 161 for Simple Network Management Protocol (SNMP).

- Monitor/Address unauthorized assets for removal, quarantine, or not allowing access to begin with.

- Manage network devices using multi-factor authentication (MFA) and encrypted sessions.

It is important to not only consider restricting traffic from certain domain names, and certain ranges of IP addresses, but also disabling the ports that are not needed to support the mission (i.e., port-filtering). However, it is important to note that in some cases, even ports that an organization believes are necessary for operation may be too dangerous. For example, password attacks against exposed remote desktop protocol (RDP) services (e.g., Port 3389) are now extremely common. If an organization needs remote desktop services, another solution should be considered first, such as requiring Virtual Private Network (VPN) to reduce risk with connections outside of the network.

Understanding the network baseline is fundamental to the security plan, and managing configuration changes over time is covered by ***CIS Control 11:*** *Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches.* Attackers look for vulnerabilities, particularly in default settings, to gain access to the network and related systems. ***Control 11*** outlines the Identifying, Detecting, and Protecting of the TMC network. For instance, sub-control 11.2 calls for *identifying*/documenting the reasons why a configuration rule is in place to allow certain traffic to flow through the network. As business needs change, the documentation will be incredibly helpful to purge configuration rules that are no longer needed and prevent unnecessary impacts on those that are needed (when documentation does not exist). It is common for TMCs to share information with other TMCs as well as to gather information from others. Documenting how this data gets into or leaves from the network is particularly important for TMCs that use Internet-based gateway portals to other systems such as:

- Remote access to a signal system or an adjacent agency's systems (e.g., 511).
- Dashboarding of public information used in transit/transportation systems.
- Digital video sharing access/controls.

Data categorization, loss prevention, and privacy considerations are discussed in more detail at the end of this chapter and should also be considered.

Further, sub-control 11.3 focuses on *detection* and the use of automated tools to compare network device configurations with known/approved configuration settings and to alert when deviations are found. As a final example, sub-control 11.4, which is crucial to all 3 implementation groups, is focused on *protection* by ensuring that stable security updates are rolled out on all network devices. Further, network separation (sub-control 11.7) is a key strategy for isolating at-risk systems from core/enterprise systems.

Much of what TMCs previously managed consisted of low-speed field devices with a variety of proprietary communication protocols. Field equipment today now includes mostly standards-based networkable appliances/devices. While there are separate initiatives focused on securing the field cabinet/network environment, the TMC Information Technology (IT) environment needs to consider these as a risk/threat vector and apply controls mentioned above to limit the types of ports and protocols traversing into the "enterprise" network from the field. As such, the TMC IT environment needs to take into consideration these basic informational components of the field networks and their impact on configuration rules at boundaries (i.e., firewalls, routers, VPN devices, etc.):

- Inventory tracking to include operating system (OS) and patch level plus firmware.
- Password management practices for technicians and devices (as appropriate); length, multi-character, and multi-factor authentication usage.
- Allocation of network segmentation via Virtual Local Access Network (VLAN) in the field and the associated impact on firewall/network configuration rules, as well as the isolation of copiers/printers and security system cameras/components.
- Securing and encrypting wireless technologies with access to the field and enterprise network.

RELEVANT CONTROLS FOR CONNECTIVITY

- *CIS Control 9: Limitation and Control of Network Ports, Protocols, and Services.*
- *CIS Control 11: Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches.*
- *CIS Control 12: Boundary Defense.*
- *CIS Control 15: Wireless Access Controls.*

Additionally, if the TMC is subject to controls associated with credit card processing back-end systems, beyond ***CIS Control 11***, network separation guidelines from Payment Card Industry Data Security Standards (PCI-DSS) also should be referenced: *Information Supplement: Guidance for PCI-DSS Scoping and Network Segmentation. December 2016.*[16] PCI-DSS is only required for handling credit card transactions.

Building upon configuration and policy controls associated with traffic passing through network devices is next supplemented by incorporating elements of ***CIS Control 12:*** *Boundary Defense,* to manage the trust levels and information flowing between networks. Similar to CIS Control 11, Control 12 covers a wide range of strategies for identifying, detecting, and protecting the network. Two of the most relevant to all organizations are sub-controls 12.3 and 12.4, which call for denying communications with known malicious Internet Protocol (IP) addresses (i.e., ranges, domain names, and/or foreign countries) as well as unauthorized Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) ports at each network boundary point. It should be noted, however, that when rolled too aggressively IP address range filtering can cause some applications to break, particularly in a "poll" and "response" system that requires openings both going out and coming back in to the network from the field.

[16] PCI Security Standards Council, "PCI Data Security Standard (PCI-DSS) Information Supplement: Guidance for PCI-DSS Scoping and Network Segmentation," 2017. Retrieved from: https://www.pcisecuritystandards.org/documents/Guidance-PCI-DSS-Scoping-and-Segmentation_v1_1.pdf.

At this point within the CIS Top 20 controls, more advanced/sophisticated strategies are more apparent, such as intrusion detection systems (sub-control 12.6) and scanning enterprise devices remotely logged in for adherence to security policies (sub-control 12.12). More sophisticated strategies will need to be prioritized for the organization based on self-assessment of areas of the greatest risks/threats. Many of these strategies will require more data collection and analysis using industry available protocols like NetFlow to collect and log data, and tools to quickly filter the data and alert on deviations from accepted standards.

Controlling physical access to wiring closets, network switches, and unused ports is primarily addressed by the aforementioned CIS Controls, but wireless access presents its own challenges warranting ***CIS Control 15:** Wireless Access Controls.* Control 15 covers securing use of wireless LANs, access points, and end-user client systems. Additionally, it covers elements such as scanning for unauthorized wireless access points connected to the network (sub-control 15.2). These are devices that are not setup according to the agency's security guidelines and represent an elevated risk for unauthorized access that bypasses back-end network authentication systems. Enforcing encryption of wireless data transmissions is a foundational control (sub-control 15.7) that applies to all implementation groups to further protect data even if the wireless signal is intercepted. Similarly, in the age of bring-your-own-device (BYOD) into the TMC environment, sub-control 15.10 is highly recommended to create a separate wireless network for untrusted devices that are primarily granted access to the Internet, but not the enterprise network.

CHAPTER 8. GUIDELINES FOR CONTROLLING STAFFING/TRAINING-RELATED ATTRIBUTES (INSIDER VULNERABILITIES)

The next two sections of this chapter pertain to the personnel component of controlling and mitigating risk through methods such as limiting the use of administrative privileges, training staff regarding security awareness initiatives, and account monitoring.

ORGANIZATION-RELATED ATTRIBUTES

With a smaller organization, it is more likely to have a small number of staff to coordinate with and track activities on a personal level when system configuration changes are noticed. In a larger Traffic Management Center (TMC), where multiple personnel, and potentially multiple shifts are available, isolating who has access and authorization to make changes to systems and the network is important for troubleshooting and follow-up after an event occurs.

Controlling the use of Administrative Privileges and the use of automated logging and monitoring (***Center for Internet Security (CIS) Controls 4, 6,*** and ***CIS Control 16)*** is critical for TMCs. This not only pertains to administrative privileges for operating systems, but logging TMC application configuration settings, logging network device configuration changes, and controlling access to network infrastructure (e.g., server data centers, network wiring closets). TMCs commonly have an array of databases gathering and storing information about traffic sensors, incident management, lane/road closures, work zones, and in some cases video recordings. Manipulation of these databases and/or the deletion of this data can have a major impact on the organization. As such, protected logging of operating systems, network device configurations, databases, and data center equipment plays an important role in data loss prevention discussed at the end of this chapter. Limiting administrative privileges to only those with a legitimate business need reduces the attack surface and the potential for inadvertent changes to these systems.

Many TMCs have contract employees supplementing their own staff. To maintain control of the TMCs in this scenario will restrict what portions of the network and applications these individuals can access, particularly restricting from accessing the enterprise portions of the network. TMCs should not solely rely on contract employees for administrative privilege control of hardware and software and network devices. Contract employees with a higher level of responsibility within the TMC should be vetted and put through appropriate background checks (Relevant to ***CIS Control 14:*** *Controlled Access Based on the Need to Know*). Restrictions on changing automated logging should be managed by TMC organization staff, or at the very least limiting those with the capability to make those changes.

RELEVANT CONTROLS FOR STAFFING

- *CIS Control 4: Controlled Use of Administrative Privileges.*
- *CIS Control 6: Maintenance, Monitoring and Analysis of Audit Logs.*
- *CIS Control 16: Account Monitoring and Control.*

Agencies also should consider incorporating policies and practices to routinely scan ports for use of disabled and outdated credentials. All these policies and practices are found to be the most reliable when they are incorporated into the workflow between groups (e.g., human resources and information technology).

TRAINING/EDUCATION

RELEVANT CONTROLS FOR TRAINING

- *CIS Control 17: Implement a Security Awareness and Training Program CIS.*

It is important for organizations to raise awareness of cybersecurity and potential threats and offer training to reinforce how to protect users, systems, and data. Most organizations have multiple teams leveraging internal training programs and lack the ability for consolidated reporting at an organizational level. To provide a holistic view into employee training it is recommended that a Learning Management System (LMS) be leveraged to provide organizations with a single console easily accessed anywhere, and a reporting tool for organizations and employees to participate in training, track progress, and report on overall organizational requirements. After identifying skills gaps, and threat vectors that require an awareness among employees, the LMS can be used to roll out training initiatives in a timely fashion and monitor compliance. (Relevant to ***CIS Control 17:*** *Implement a Security Awareness and Training Program.*) TMCs that manage Industrial Control Systems, such as SCADA networks for tunnels, are encouraged to further supplement the CIS Controls with section 6.2.2 of National Institute of Standards and Technology (NIST) 800-82r2, and NIST 800-50.[17]

For TMCs with limited training staff or funding available to provide training, third-party training services and programs are available and should be explored. The following table contains a list of common or popular training sources that may be applicable to security staff with responsibilities in TMC environments that include aspects of industrial control system (ICS)/ SCADA infrastructure.

[17] NIST, "SP 800-50 Building an Information Technology Security Awareness and Training Program," 2003. Retrieved from: https://csrc.nist.gov/publications/detail/sp/800-50/final.

Table 1. List of industrial control systems-related training.

Source	Type	Free?	Topics
ICS-CERT[a]	Web-based	Yes	• Operational Security (OPSEC) for Control Systems (100W)—1 hour. • Differences in Deployments of ICS (210W-1)—1.5 hours. • Influence of Common Information Technology (IT) Components on ICS (210W-2)—1.5 hours. • Common ICS Components (210W-3)—1.5 hours. • Cybersecurity within IT and ICS Domains (210W-4)—1.5 hours. • Cybersecurity Risk (210W-5)—1.5 hours. • Current Trends (Threat) (210W-6)—1.5 hours. • Current Trends (Vulnerabilities) (210W-7)—1.5 hours • Determining the Impacts of a Cybersecurity Incident (210W-8)—1.5 hours. • Attack Methodologies in IT and ICS (210W-9)—1.5 hours. • Mapping IT Defense-in-Depth Security Solutions to ICS (210W-10)—1.5 hours.
ICS-CERT	Instructor-led	Yes	• Introduction to Control Systems Cybersecurity (101)—8 hours. • Intermediate Cybersecurity for Industrial Control Systems (201)—8 hours. • Intermediate Cybersecurity for Industrial Control Systems (202)—8 hours. • ICS Cybersecurity (301)—5 days.
SANS[b]	Multiple	No	• ICS410: ICS/SCADA Security Essentials. • ICS456: Essentials for North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection. • ICS515: ICS Active Defense and Incident Response.
FedVTE[c, d]	Web-based	Yes	Federal Virtual Training Environment (FedVTE): • 101 Critical Infrastructure Protection—2 hours.

[a] NCCIC/ICS-CERT, "Training Available Through ICS-CERT." Retrieved from: https://ics-cert.us-cert.gov/Training-Available-Through-ICS-CERT.

[b] SANS, "Cyber Security Courses." Retrieved from: https://www.sans.org/courses/.

[c] FedVTE, "FedVTE Course Catalog." Retrieved from: https://fedvte.usalearning.gov/coursecat_external.php?group=ALL

[d] Appears to be limited to Federal employees only.

(Source: Federal Highway Administration.)

The *National Initiative for Cybersecurity Careers and Studies (NICCS) Catalog* provides a list of cybersecurity courses of all topics from a wide variety of sources.[18] It can be used to find relevant courses, and vendors that are local with respect to a given organization.

Employee Exit Process

An essential/basic element of asset control is the removal of account credentials from an employee at the time of departure. Based on the risk management plan for an organization and/or the sensitivity of certain applications and data, a TMC agency might exercise restricted access to some systems before departure. At a minimum, when given notice of an individual's impending departure, lowering their access privileges down to an appropriate "need-to-know" level and revoking full administrative privileges is consistent with guidelines in ***CIS Control 14:*** *Controlled Access Based on the Need to Know* and ***CIS Control 4:*** *Controlled Use of Administrative Privileges*, respectively.

All agency-owned assets loaned to the employee for use should be asset-tagged and returned to the agency as part of the Exit Process. Any software that requires special dongles or keys to access also should be covered by asset management tracking tools and incorporated into the checklist of items to be returned during the Exit Process. Field cabinet access keys/devices also need to be returned.

After considerations for Federal (36 CFR 1220.14), State, or local recordkeeping requirements, agencies should incorporate policies for sanitizing and/or disposing of electronics (e-disposal), personal information/folders.[19] It is recommended that any electronics sent out for e-disposal be sanitized beforehand or contracted through a reputable service provider who will be destroying the media altogether. While this is a critical time to deal with e-disposal upon employee exit, this is a broader organizational issue that is worth incorporating into routine e-sanitization policies for risk management practices, and data protection that is discussed below.

[18] National Initiative for Cybersecurity Careers and Studies (NICCS), "NICCS Education and Training Catalog." Retrieved from: https://niccs.us-cert.gov/training/search.

[19] National Archives and Records Administration (NARA), "NARA Code of Federal Regulations." Retrieved from: https://www.archives.gov/about/regulations/regulations.html.

CHAPTER 9. GUIDELINES FOR RESILIENCY/DATA PROTECTION AND RECOVERY

INTERAGENCY INFORMATION SHARING AND COLLABORATION

When developing cybersecurity guidelines, it is important for agencies to work together to share past experiences and best practices. These partnerships can be between organizations within the same agency (e.g., a localities Information Technology (IT) department and Public Works) and among agencies within the same industry (e.g., local and State Traffic Management Centers (TMC)). This will help build an awareness of industry risks and standards and ensures that the most innovative approaches are being utilized and expanded upon industry-wide. These partnerships also can serve as a platform for discovering and applying for Federal resources and incentives.

In 2013, the Department of Homeland Security (DHS) in collaboration with the critical infrastructure community developed the National Infrastructure Protection Plan (NIPP) titled *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience* which serves as a guide for the national effort to manage risk to critical infrastructure as a collaborative effort. This document presents shared national vision, mission, and goals with respect to managing risk and serves as a guideline for organizations or groups of organizations to develop a collaborative partnership.[20]

Another platform for developing partnerships that TMCs should consider is any of various applicable Information Sharing and Analysis Centers (ISAC), which are sector-based, non-profit limited liability companies (LLC) developed to help companies across industries collaborate and coordinate via the National Council of ISACs (NCI).[21] Some examples that may be of interest to TMCs include:

- Surface Transportation, Public Transportation and Over-The-Road Bus ISACs.
- Emergency Management and Response ISAC.
- Information Technology ISAC.[22]

RELEVANT CONTROLS FOR COLLABORATION

- *CIS Control 4: Controlled Use of Administrative Privileges.*
- *CIS Control 14: Controlled Access Based on the Need to Know.*

[20] Department of Homeland Security (DHS), "NIPP 2013: Partnering for Critical Infrastructure Security and Resilience," 2013. Retrieved from: https://www.dhs.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf.

[21] National Council of ISACs (NCI). Retrieved from: https://www.nationalisacs.org/member-isacs.

[22] The Information Technology—Information Sharing and Analysis Center (IT-ISAC). Retrieved from: https://www.it-isac.org/.

Additionally, IT-ISAC has developed industry Special Interest Groups to combine peer member companies within similar industries, such as the Food and Agriculture industry. A TMC would benefit by being an active member of the ISAC where indicators of compromise or events of interest could be shared within their sector and could lead the development of a TMC or Transportation Industry special interest group. When agencies/parent organizations belong to multiple ISACS, communications should be coordinated within the parent organization to establish a protocol for managing communications with the various ISACS to prevent duplicate or conflicting communications.

Each of these sample ISACs was developed to help companies across each associated sector manage risks through information sharing and analysis.

Risk Management Plan

Building upon the individual predecessor efforts above for TMCs that are lacking a risk management plan, the figure from *NIPP Supplemental Tool: Executing A Critical Infrastructure Risk Management Approach* provides a concise path to support those that are beginning to implement a risk management approach to cybersecurity to incorporate aspects of the *National Institute of Standards and Technology (NIST) 800-37 Guide for Applying the Risk Management Framework*. It is unrealistic to expect complete prevention of all vulnerabilities. Risk analysis is used to identify where the greatest risks/weaknesses exist, and a risk management plan is used to determine courses of action to mitigate and manage those risks.

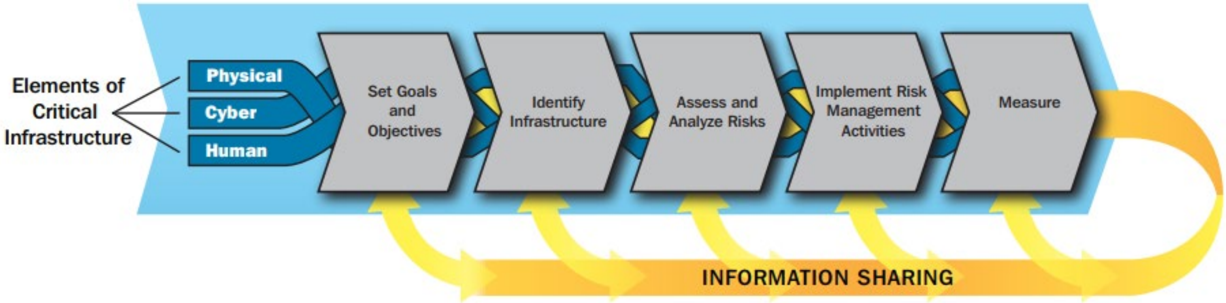


Figure 10. Flowchart. The National Institute of Standards and Technology 800-37 risk management approach.
(Source: NIST 800-37 Guide for Applying the Risk Management Framework.)

Related to the figure above, within the previous sections of this report, inventory and identification of hardware, software and network elements in the TMC has been reviewed to satisfy the Identify Infrastructure component of this process. For TMC/organizations that are unfamiliar with performing risk assessments, *NIST 800-30* is a *Guide for Conducting Risk Assessments*.[23] For the TMC environment, organizations should directly assess the risk and impact of a field equipment breach, an operator workstation breach, a server breach, a network

[23] NIST, "SP 800-30 Rev. 1 Guide for Conducting Risk Assessments," 2012. Retrieved from: https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final.

access breach, and the categorization of the data systems that are the most critical to daily operations.

The outcome of the risk analysis will allow the TMC management the ability to develop risk-based security governance for the risk management plan, setting goals/objectives, and implementing risk management activities. Throughout the process, information would be fed back to support follow-up activities and engaging collaboration with IT and Operations Technology (OT) staff.

While Center for Internet Security (CIS) Controls noted up to this point all play a part in an agency's overall risk management strategy, the following activities relate specifically to the Measure portion of the risk management approach process flow by evaluating the performance of organizational plans/strategies. The intent is to establish a program that is fundamentally part of the agency's routine processes.

- As the TMC environment's skillset matures and the level of sophistication warrants it, ***CIS Control 20:*** *Penetration Tests and Red Team Exercises* are recommended to be incorporated for TMCs in implementation groups 2 and 3. Factoring these tests into the overall risk management plan will improve the overall resiliency of the TMC by proactively identifying and mitigating vulnerabilities. The most common areas of concern in a TMC environment involve wireless access networks, Internet connectivity, and connections to field network devices. Penetration and Red Team exercises are conducted less frequently than other CIS Controls, typically annually.

RELEVANT CONTROLS FOR RISK MANAGEMENT

- *CIS Control 3: Continuous Vulnerability Management.*
- *CIS Control 20: Penetration Tests and Red Team Exercises.*

- Payment Card Industry (PCI) compliance testing should be incorporated if applicable to the TMC. Typically, testing is performed annually.

- Cybersecurity is not a once and done situation. It must be continually monitored, managed and refined as the threats continue to evolve. ***CIS Control 3:*** *Continuous Vulnerability Management* provides key ways to incorporate vulnerability assessment, protection, and responsiveness into routine processes. This ranges from deploying automated software patch management tools (sub-control 3.5) to automated vulnerability scanning tools (sub-control 3.1).

Cybersecurity is not a once and done situation. It must be continually monitoring, managed and refined as the threats continue to evolve.

All guidelines suggest every agency should complete a formal risk assessment and develop their own resiliency plan. However, low levels of resources can make this challenging, especially in the preliminary stages of plan development. As many of the best practices identified above should be implemented at a minimum using CIS Top 20 and NIST Framework as a baseline.

Incident Planning and Response

Relevant Controls for Incident Planning and Response

- *CIS Control 19: Incident Response and Management.*

It is not a matter of whether systems will encounter a threat, but when. In preparation for this occurrence, ***CIS Control 19:*** *Incident Response and Management* recommends the development of an Incident Response Plan. The Incident Response Plan describes an approach for responding to information security incidents. It defines the roles and responsibilities of personnel, characterization of incidents, communication plans, and reporting requirements. The goal of the Incident Response Plan is to provide guidelines to manage the response process in an effective and consistent manner.

The document also should reference the organization's Business Continuity Plan to appropriately categorize critical assets which assist in assigning severity levels to incidents. This also will help organizations work toward the development of organization-wide incident reporting standards with respect to time allowances, means and methods, and reporting requirements (e.g., whether the incident should be reported to an individual within the organization or third-party authorities).

The document should be written down for ease of access and should be used to train incoming staff. It is intended that this will be a living document to be modified to incorporate industry risks and best practices as they change. As part of this ongoing revision, an industry best practice is to execute periodic table top exercises to test the Incident Response Plan. The results of these exercises will help organizations identify gaps and outlying vulnerabilities and fine-tune their response procedures. The CIS Controls identify the actions that are recommended for an effective Incident Response and Management control, but specific examples are not provided. This is where NIST documentation is a useful supplement to implementing the CIS Controls since reference samples are available to be modified and tailored to an organization's unique needs and requirements.

Sample Incident Response Process: The National Institute of Standards and Technology Incident Lifecycle

The Computer Security Incident Handling Guide (NIST SP 800-61r2) identifies the Incident Response Life Cycle by expressing it in four phases:[24]

- Preparation.
- Detection and Analysis.
- Containment, Eradication, and Recovery.
- Post-Incident Activity.

[24] NIST, "SP 800-61 Rev. 2 Computer Security Incident Handling Guide," 2012. Retrieved from: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf.

Preparation: Preparation involves preparing to respond to potential incidents, by assembling personnel, developing training, and gathering the necessary hardware and software to accommodate the incident responses. During the Preparation phase systems, networks, and applications also are kept secure through the continuous monitoring for anomalous traffic and the tracking and patching of system and application vulnerabilities.

The CIS Controls identify the actions that are recommended but specific examples are not provided. This is where *NIST documentation is a useful supplement to implementing the CIS Controls* since reference samples are available to be modified and tailored to an organization's unique needs and requirements.

Detection: The Detection and Analysis phase is the discovery of an event with security tools or notification by an employee, inside party or outside party about a suspected incident. During this phase the team seeks to determines the priority, scope, risk and root cause of the incident. This phase includes the creation of a ticket with appropriate classification to begin identifying the details of the event. It is important to identify the initial vector, and what data, systems, employees, or regions were affected. A crucial step in this phase is the evidence gathering and handling to help document and preserve a chain of custody for legal proceedings.

The Containment, Eradication, and Recovery: The Containment, Eradication, and Recovery phase is the triage phase where the Incident Response Team's primary objective involves preventing further damage to the victim organization and eliminating remnant of the unauthorized activity from the affected systems. Strategies will vary depending on the incident so it is important to have these strategies pre-determined to help facilitate decision-making.

Post-Incident: Post-Incident Activity is critical to improving response sharing lessons learned with all teams involved. It is important to hold these meetings within a few days of the end of an incident. Refer to NIST SP 800-61r2 section 3.4.1 Lessons Learned for more information on what the meeting discussion should include.

Resiliency Plan

Incrementally building a more robust process/program for resiliency is the purpose for developing a resiliency plan to harden systems and facilities to improve the ability to recover from an attack or breach. The technical publication by MITRE titled *Cyber Resiliency Design Principles/Selective Use Throughout the Lifecycle and in Conjunction with Related Disciplines* dated January 2017 is a resource for aiding in the development of a resiliency plan and design for TMC IT environments.[25]

The following figure from the MITRE publication shows the relationships and building blocks related to resiliency goals evolving into objectives and ultimately techniques to improve the

[25] MITRE, "Cyber Resiliency Design Principles: Selective Use Throughout the Lifecycle and in Conjunction with Related Disciplines," 2017. Retrieved from: http://www.mitre.org/sites/default/files/publications/PR%2017-0103%20Cyber%20Resiliency%20Design%20Principles%20MTR17001.pdf.

resiliency of the TMC systems and network environment. Establishing layered defenses is a widely used resiliency strategy relevant to TMCs, particularly when coupled with segmentation/isolation strategies already discussed in this report. The technique most often used by TMCs involves Redundancy (of software, hardware, network equipment, configuration backup files, off-site recovery equipment/locations). Many of the remaining techniques are more sophisticated and thus more applicable to implementation groups 2 and 3. A Resiliency Plan is intended to look at how each of these techniques could be used to address the agency's ability to withstand and mitigate a given threat to the continuity of their operations.

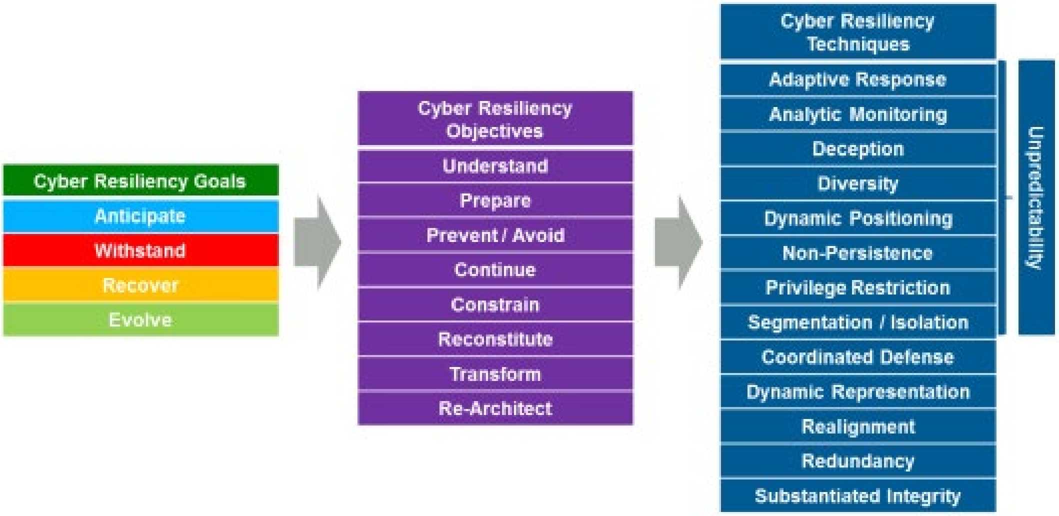


Figure 11. Flowchart. Cyber resiliency engineering framework.
(Source: Cyber Resiliency Design Principles/Selective Use Throughout the Lifecycle and in Conjunction with Related Disciplines, MITRE.)

When responding and recovering from a breach or widespread application failure, the TMC's resiliency plan should contain a prioritization plan for restoring applications in order of greatest criticality. Recovery times and frequency of backups (discussed below) will impact storage capacity and techniques, which should in turn be folded into system upgrade plans for future upgrades.

Resiliency plans for TMCs should contain strategies for central device authentication, malware protection strategies for standard devices, and network segmentation of devices that cannot be controlled at an acceptable level to achieve agency cybersecurity goals. For example, a resiliency plan could account for devices that do not support central authentication and are segmented in the network from others such that just one segment can be temporarily shut off/disconnected in the event of a breach. This type of strategy is an example of how to improve the response time and continuity of operations for an organization's resiliency to an incident.

Any opportunity to reduce the TMC's potential attack surface by reducing open ports and protocols passing between networks should be employed and actively incorporated into the TMC's Resiliency Plan. Finally, as a general guide for developing the Plan, evaluate the least level of privileged access that can be used to satisfy each objective to prevent unnecessarily high-level access to devices or systems.

Malware Defenses

One specific form of system and data protection that should be included in an agency's Resiliency Plan is malware protection. Part of that Plan should include monitoring known sources of credible information about known threats and vulnerabilities. The Cybersecurity and Infrastructure Security Agency (CISA) incorporates an industrial control system (ICS) element into their Computer Emergency Response Teams (CERT) and posts routine alerts and advisories on their website, which also can be subscribed to via a Really Simple Syndication (RSS) feed.[26] Malicious software is a widespread threat across the cyber world that can enter through any number of points such as end-user devices, email attachments, webpages, cloud services, user actions, and removable media. For the TMC world, these entrances can include not only staff daily operations but field devices as well. This agility paired with the speed at which attacks occur and spread make malware a priority risk to protect against with a dedication to keeping the protection current.

CIS Control 8: Malware Defenses provides guidelines on controls to implement and manage malware protection including monitoring and removal. With respect to document control, anti-malware software with anti-exploitation features should be a fundamental consideration to protecting TMCs from malware infiltration as well as data loss from malware infiltration. In addition to scanning emails at the server level, or network traffic passing through the firewall, at the very least implementation groups 2 and 3 also should utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers (sub-control 8.1). All organizations also are strongly recommended to set operating system policies that prevent auto-running applications (sub-control 8.5) held on removeable media devices (e.g., flash drives, camera memory cards, CDs, etc.).

RELEVANT CONTROLS FOR DATA PROTECTION

- *CIS Control 13: Data Protection.*

Data Loss Prevention

TMCs manage copious amounts of data from incident management logs to the massive amounts of traffic sensor data and crowd-sourced data that has both real-time and historical value for operations managers. TMC operators may have experienced the loss of that data from storage device failures, accidental deletion (by users with system privileges set too high), malware that blocks access to servers/data, and/or a corrupt field device that overwrites the central database. However, data theft is the primary focus of CIS Control 13, which is described below. Understanding the importance and value of the TMCs datasets is the first step in data loss prevention.

Data loss prevention (DLP) refers to a procedure or policy for monitoring and detecting unauthorized data breach and exfiltration attempts by monitoring, detecting, and blocking

[26] Cybersecurity and Infrastructure Security Agency Industrial Control Systems Alerts and Advisories. Retrieved from: https://ics-cert.us-cert.gov/.

sensitive data. *CIS Control 13: Data Protection* provides guidelines for DLP techniques. As a first step, it is important for organizations to identify and classify their data. Best practice is to create at least 3 and optimally no more than 5 basic data labels: Create a "General" label that is default (applied to everything) allowing the user to upgrade to a higher classification (e.g., Operations, Supervisory Control and Data Acquisition (SCADA), Sensitive/PCI), or downgrade to a lower classification with explanation.

DLP is a best practice to implement on specific use cases, however sifting through alerts can consume considerable man hours. As an alternative to manually filtering and processing data, commercial DLP solutions are available for purchase and deployment by organizations with limited staff availability. Use-cases for DLP include monitoring for specific data/file types and tags in files or unauthorized use of encryption of files located on the network that have been identified as threats/vulnerabilities by ICS-CERT or others, along with monitoring significant data transmissions outside of the network. Organizations should still plan at a minimum to dedicate staff to reviewing the event logs regularly and following up on events related to attempts to transmit sensitive information without authorization, as well as to tune the tools to manage the volume and types of alerts that are of no consequence or value to reduce considerable person hours required to implement DLP.

Information Rights Management (IRM) are features for document creation that can enforce encryption on all newly created documents and protect files from unauthorized copying, viewing, printing, forwarding, deleting, and editing as an added layer of protection. This allows the document owner to place the correct label (data classification) plus security attributes that could set a timeframe on a document to limit viewing, provide the ability to revoke the document, and prevent the ability to print or forward on to another user. To achieve further data tracking and control, organizations should implement a management system capable of tracking client/user data as well.

Archival/Backup, Restoration, Recovery

If the organization had to start from scratch to recreate the network and digital files tomorrow, does the organization have what it takes? Nightly backups may not be frequent enough for real-time data gathering in a TMC environment. Many TMCs and business IT enterprises have recognized that the loss of certain data sets is too critical to rely solely on nightly backups. For some organizations, device configuration settings and maintenance/repair history changes frequently enough that backing up the files every hour is an appropriate frequency, while for others a nightly backup is sufficient. TMC incident logs, traffic sensor data, and dynamic message sign logs/schedules are elements of operations that would suggest real-time replication to a secondary database server, preferably in a separate physical location. TMCs also should consider external users that rely on information published or transmitted by the TMC. Road closure and incident status information are both real-time indicators that motorists and third-party mapping applications now routinely rely on, and that should have an appropriate level of redundancy and frequency of backups.

Whether part of risk analysis, or a separate enterprise business impact analysis, TMCs should determine the acceptable frequency of backup recovery points and recovery times to maintain continuity of operations based on organizational objectives. As previously discussed under **Incident Planning and Response**, data restoration and recovery are key components of the incident response process. Doing so without continuing to compromise the network by restoring corrupt or infected data, while also maintaining as much of the data as possible and limiting data loss, is an equally important aspect of data recovery. Part of the response plan should include a procedure to test the backups for existence of malware or other corruption before restoring infected files and causing further issues. Maintaining at least one backup offsite is a technique used to isolate both the primary and the backup from being infected.

Step one in preparing for data restoration and recovery is data backup. Backup types include mirror, full, incremental, and differential. Organizations should analyze the pros and cons of each type of backup to determine the best or most realistic backup schedule by type. Organizations should strive for automated, routine data backup. Once a data backup schedule has been determined, it is important to remember that backup data can quickly take up space on an organization's server and should be accounted for. An organization's policies should include requirements with respect to data backup retention and disposal. Much of this will stem from regulation, legal requirements, or contractual obligations, such as PCI.

For the sake of organization efficiency, it is important that data recovery is also completed in a timely manner. As briefly indicated under **Incident Planning and Response**, organizations should perform a Business Impact Analysis (BIA) prior to creating a Recovery Point Objective (RPO) and Recovery Time Objective (RTO)—the time it takes to restore data prior to the disruption and the functional restoration of a business service post disruption—to ensure that higher recovery priority is given to data with a higher impact on the organization's functionality.

To verify backup system integrity without risking data loss, organizations should regularly test the system's backup and restoration process on a sample of data in a test bed environment. ***CIS Control 10:** Data Recovery Capabilities* recommends performing such tests once per quarter, or whenever new backup equipment is purchased, whichever comes first.

Bacula Systems provides additional information about data backup best practices, along with examples with respect to labeling, schedules and retentions, partitioning, and recovery plans.[27]

Personal Privacy Information Legislation

Personal information privacy continues to gain more widespread attention. The European Union (EU) established a law pertaining to general data protection regulation (GDPR) to govern the control that individuals have over their personal data. Additionally, similar legislation passed in the State of California called the California Consumer Privacy Act, which takes effect in January 2020. There are groups lobbying/advocating for taking privacy legislation/initiatives to the Federal level. TMCs subject to these requirements should monitor the impacts of this legislation on their own systems that contain personal information from dashboard users, 511 users, or other traveler information systems at a minimum. Data from these users should be scrubbed from

[27] Bacula Systems, "Enterprise Data Backup Best Practices (Prior to installation)." Retrieved from: https://www.baculasystems.com/enterprise-data-backup-best-practices.

backups and protected from the Federal Information Processing Standards (FOIA) requests at a minimum. Many TMCs now get incident alerts/data from State and local police agencies. If that data has not been pre-sanitized to remove personal information before use in the TMC incident management databases, then it should be sanitized by the TMC and scrubbed from archives/ backups as well. As noted above with respect to DLP, agencies should consider a category of data related to personal privacy data that be screened or quickly isolated within the broader context of the agency's wide array of data.

CHAPTER 10. SHORT- AND LONG-TERM STRATEGIES FOR ADDRESSING ISSUES/GAPS

The Traffic Management Center (TMC) operators manage a large volume of data, which is largely real-time, whereby data losses have significant consequences for their organization as well as others that rely on them. As part of the country's critical infrastructure, TMCs need to assess and classify the criticality of the different datasets that are collected or generated within the TMC as noted previously as a key step for determining steps for data loss prevention. Additionally, TMC's Operations Technology (OT) staff manage the configurations of networked field appliances, which presents a challenge similar to those directly in the industrial controls (i.e., Supervisory Control and Data Acquisition (SCADA)) industry. Handling networked OT equipment (e.g., sensors, signal controllers, message sign controllers, etc.) that does not follow upgrade cycles at the same frequency as the Information Technology (IT) industry requires a different level of care than a traditional business data center to mitigate potential risks in a TMC. TMCs also have exposure to insider vulnerabilities with respect to operators that are subject to social engineering attacks, poor cyber-hygiene, or simply no limitations on what data and controls that operators have access to. This is one of the reasons that approved message libraries for dynamic message signs were established by many organizations to prevent rogue messages being deployed by disgruntled operators and/or hackers that gainfully access the system.

When facing a large obstacle/challenge it can be daunting to know what part to tackle first. Fortunately, the Center for Internet Security (CIS) Controls has been segmented into Basic, Foundational, and Organizational controls of increasing complexity and sophistication. Equally, the sub-controls are organized into implementation groups (1, 2, and 3) for prioritization for organizations of increasing size and sophistication. Based on observations from industry data and results from the questionnaires, in the short-term TMC operators should focus on implementing all the Basic CIS Controls, along with Foundational Controls that address the greatest vulnerabilities to the respective organization based on risk analysis.

It is recommended that agencies conduct a self-assessment, if one already has not been performed, that can provide guidelines on which Foundational and Organizational controls are the most critical to the organization. With that information in hand, the organization can use the priorities within the CIS sub-controls to focus on the outcomes for the associated Implementation Group for the areas of highest risk.

The Department of Homeland Security (DHS) has developed a self-assessment Cybersecurity Resilience Review (CRR) tool based on the National Institute of Standards and Technology (NIST) for State, Local, and Tribal governments, and provides a performance measurement for the individual completing the evaluation with respect to 10 categories based on responses to a series of questions within each category.[28] A list of these categories is provided below, connected to the associated CIS Controls for context. This assessment may be conducted as a self-assessment, or as an on-site assessment facilitated by DHS if preferred.

[28] Department of Homeland Security (DHS), "Cyber Resilience Review (CRR): Self-Assessment Package," 2016. Retrieved from: https://www.us-cert.gov/ccubedvp/assessments.

1. Asset Management:
    - *CIS Control 1: Inventory and Control of Hardware Assets.*
    - *CIS Control 2: Inventory and Control of Software Assets.*
    - *CIS Control 4: Controlled Use of Administrative Privileges.*
    - *CIS Control 9: Limitation and Control of Network Ports, Protocols and Services.*
    - *CIS Control 12: Boundary Defense.*
    - *CIS Control 13: Data Protection.*

2. Controls Management:
    - *CIS Control 4: Controlled Use of Administrative Privileges.*
    - *CIS Control 9: Limitations and Control of Network Ports, Protocols and Services.*
    - *CIS Control 14: Controlled Access Based on the Need to Know.*
    - *CIS Control 15: Wireless Access Control.*
    - *CIS Control 16: Account Monitoring and Control.*

3. Configuration and Change Management:
    - *CIS Control 4: Controlled Use of Administrative Privileges.*
    - *CIS Control 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers.*
    - *CIS Control 6: Maintenance, Monitoring and Analysis of Audit Logs.*
    - *CIS Control 10: Data Recovery Capabilities.*
    - *CIS Control 13: Data Protection.*
    - *CIS Control 14: Controlled Access Based on the Need to Know.*

4. Vulnerability Management:
    - *CIS Control 3: Continuous Vulnerability Management.*
    - *CIS Control 20: Penetration Tests and Red Team Exercises.*

5. Incident Management:
    - *CIS Control 6: Maintenance, Monitoring and Analysis of Audit Logs.*
    - *CIS Control 19: Incident Response and Management.*

6. Service Continuity Management
    - *CIS Control 19: Incident Response and Management.*

7. Risk Management:
    - *CIS Control 3: Continuous Vulnerability Management.*
    - *CIS Control 6: Maintenance, Monitoring and Analysis of Audit Logs.*
    - *CIS Control 7: Email and Web Browser Protections.*
    - *CIS Control 8: Malware Defenses.*
    - *CIS Control 9: Limitation and Control of Network Ports, Protocols and Services.*
    - *CIS Control 11: Secure Configuration for Network Devices, such as Firewalls, Routers and Switches.*
    - *CIS Control 12: Boundary Defense.*
    - *CIS Control 14: Controlled Access Based on the Need to Know.*

- *CIS Control 16: Account Monitoring and Control.*
- *CIS Control 18: Application Software Security.*
- *CIS Control 20: Penetration Tests and Red Team Exercises.*

8. External Dependencies Management:
   - *CIS Control 3: Continuous Vulnerability Management.*
   - *CIS Control 4: Controlled Use of Administrative Privileges.*
   - *CIS Control 14: Controlled Access Based on the Need to Know.*
   - *CIS Control 16: Account Monitoring and Control.*

9. Training and Awareness:
   - *CIS Control 17: Implementing a Security Awareness and Training Program.*

10. Situational Awareness:
    - *CIS Control 6: Maintenance, Monitoring and Analysis of Audit Logs.*
    - *CIS Control 17: Implementing a Security Awareness and Training Program.*

Within the Self-Assessment, agencies indicate whether recommended practices within each of the above categories are not performed, incompletely performed, or performed.

Upon completion of the assessment, a report is generated summarizing the responses given. Based on the responses to each question, scores are provided for individual Practices, Goals, and Domains.

- A **Practice** is associated with each question.
- **Goals** are comprised of multiple associated Practices.
- Each category listed above is associated with a **Domain**, which is comprised of multiple associated Goals.

If all Practices within a Goal are indicated as performed, that Goal is achieved. If all Goals within a Domain are performed, that Domain is achieved, and the agency is assigned a Maturity Indicator Level (MIL1-MIL5 corresponding to 1-Performed, 2-Planned, 3-Managed, 4-Measured, and 5-Defined, further defined in the appendix) for the Domain based on answers to questions associated with Practices. For example, if all MIL1 Goals are achieved, the agency will achieve a Domain maturity level of MIL1. If additional maturity Goals are achieved, that agency will achieve a higher maturing rating indicating a higher level of performance for that Domain. If the agency does not achieve every Goal within a Domain and therefore achieve a Domain, they are assigned a maturity score of MIL0 (incomplete). A sample response and associated report results for Domain 9 Training and Awareness can be found in the appendix.

Every organization should at the very least achieve MIL1 in the short-term. Ultimately, agencies should strive to increase their maturity to MIL5 for the respective areas in their risk management plan. The self-assessment can be considered both a report card of where the agency stands, and a means to develop an action plan to address the areas having less management/maturity.

The report then provides information on how the assessment results connect to the NIST Framework, along with options to consider helping agencies achieve goals they currently are not performing along with references to the associated section within NIST to find additional guidelines. Additionally, TMCs can then focus on the CIS Controls associated with each of these Domain categories identified above. Implementation groups 2 and 3, will inherently have more areas to focus on than implementation group 1.

In the long-term, TMCs are encouraged to embrace the remaining Foundational controls and incorporate Organizational Controls to document and memorialize procedures as the agency's capability matures toward a MIL5 level. Furthermore, to provide continuous vulnerability assessment and protection, process improvement and refinement will need to continue and adapt as the industry evolves.

CHAPTER 11. CONCLUSIONS AND NEXT STEPS

Throughout these guidelines, cybersecurity issues that are unique to the Traffic Management Centers (TMC) Information Technology (IT) environment have been discussed, along with resources to assist with establishing a programmatic system to mitigate identified risks particular to an agency's TMC IT environment. The Center for Internet Security (CIS) Top 20 Controls have been covered as the most relevant framework for the operations environment in TMCs. Cybersecurity is not a one and done issue; it requires programmatic involvement on a recurring basis.

Some agencies already will have a jumpstart on cybersecurity issues, while others may be closer to starting from scratch when reading these guidelines. If an agency is starting from scratch, a *Risk Analysis* is recommended as the first step towards establishing a cybersecurity program for the TMC. As noted in chapter 10, there are resources available online such as Department of Homeland Security's (DHS) self-assessment Cybersecurity Resilience Review (CRR) tool.

With an understanding of the risks that the TMC environment is exposed to, agencies can then focus on implementing *CIS Controls* to establish and maintain a program for continuing to improve the resiliency of the TMC IT environment. The initial focus of the CIS Controls should be to address the risks that pose the most immediate concerns based on the risk analysis. For organizations that already have started embracing the National Institute of Standards and Technology (NIST) Framework and are comfortable using that guidance, the CIS Controls documented in these guidelines along with the cross-mapping tools by CIS can be helpful to gauge how mature the organization is with respect to cybersecurity risk management for basic, foundational, and organizational aspects.

In conjunction with addressing immediate risks from the Risk Analysis, TMC agencies will benefit from developing a *Risk Management Plan*, as noted in chapter 9, to determine courses of action to mitigate and systematically manage those risks.

Part of increasing the cybersecurity maturity of an agency involves incrementally building a more robust process/program for resiliency by developing a *Resiliency Plan* to harden systems and facilities to improve the ability to recover from an attack or breach.

TMC operations staff are encouraged to collaborate on the risk analysis with IT staff to establish a program that addressed both perspectives for operations functionality while mitigating risks. Developing a cooperative panel comprised of both perspectives has been noted to be beneficial for organizations, especially in advance of incident response when power struggles have been identified as more likely to occur, which then slows the recovery process. The cooperative panel of Operations Technology (OT) and IT staff should lead the charge on routinely testing and improving the program to address existing and newly identified risks. The panel is encouraged to participate in/with peer groups (i.e., Information Sharing and Analysis Centers (ISAC) as noted in chapter 9) to share and learn from identified threats/risks within the TMC community to allow all TMC operators to learn and benefit from the greater body of knowledge.

APPENDIX A. SAMPLE CYBERSECURITY RESILIENCE REVIEW SELF-ASSESSMENT

MATURITY INDICATOR LEVELS DEFINED

Maturity Indicator Levels (MIL)[29] are assigned by Domain and represent a consolidated view of performance. CERT-RMM MILs describe attributes that would be indicative of mature capabilities as represented in the model's capability levels. However, they do not fully represent capability levels as defined because a capability level can only be assigned through a formal appraisal process, not as the result of using an assessment-based instrument.

MIL0 Incomplete

Indicates that Practices in the Domain are not being performed as measured by responses to the relevant Cyber Resilience Review (CRR) questions. If MIL0 is assigned, no further assessment of maturity indicator is performed.

MIL1 Performed

Indicates that all Practices in a Domain are being performed as measured by responses to the relevant CRR questions. MIL1 means that there is sufficient and substantial support for the existence of the practices.

MIL2 Planned

Indicates that all Practices in Domain are not only performed, but are supported by sufficient planning, stakeholders, and relevant standards and guidelines. A planned process/practice is:

- Established by the organization (Is the practice documented and communicable to all who need to know?).
- Planned (Is the practice performed according to a documented plan?).
- Supported by stakeholders (Are the stakeholders of the practice known and are they aware of the practice and their role in the practice?).
- Supported by relevant standards and guidelines (Have the standards and guidelines that support the practice been identified and implemented?).

MIL3 Managed

Indicates that all Practices in a Domain are performed, planned, and have the basic infrastructure in place to support the process. A managed process/practice:

[29] Department of Homeland Security (DHS), "Cyber Resilience Review (CRR): Self-Assessment Package," 2016. Retrieved from: https://www.us-cert.gov/ccubedvp/assessments.

- Is governed by the organization (Is the practice supported by policy and is there appropriate oversight over the performance of the practice?).

- Is appropriately staffed and funded (Are the staff and funds necessary to perform the practice as intended available?).

- Is assigned to staff who are responsible and accountable for the performance of the practice (Have staff been assigned to perform the practice and are they responsible and accountable for the performance of the practice?).

- Is performed by staff who are adequately trained to perform the practice (Are the staff who perform the practice adequately skilled and trained to perform the practice?).

- Produces work products that are expected from performance of the practice and are placed under appropriate levels of configuration control (Does the practice produce artifacts and work products that are expected from performing the practice, and if so, are the configurations of these artifacts/work products managed?).

- Is managed for risk (Are risks related to the performance of the practice identified, analyzed, disposed of, monitored, and controlled?).

MIL4 Measured

Indicates that all Practices in a Domain are performed, planned, managed, monitored, and controlled. A measured process/practice is:

- Periodically evaluated for effectiveness (Is the practice periodically reviewed to ensure that it is effective and producing intended results?).

- Monitored and controlled (Are appropriate implementation and performance measures identified, applied, and analyzed?).

- Objectively evaluated against its practice description and plan (Is the practice periodically evaluated to ensure that it adheres to the practice description and the plan for the practice?).

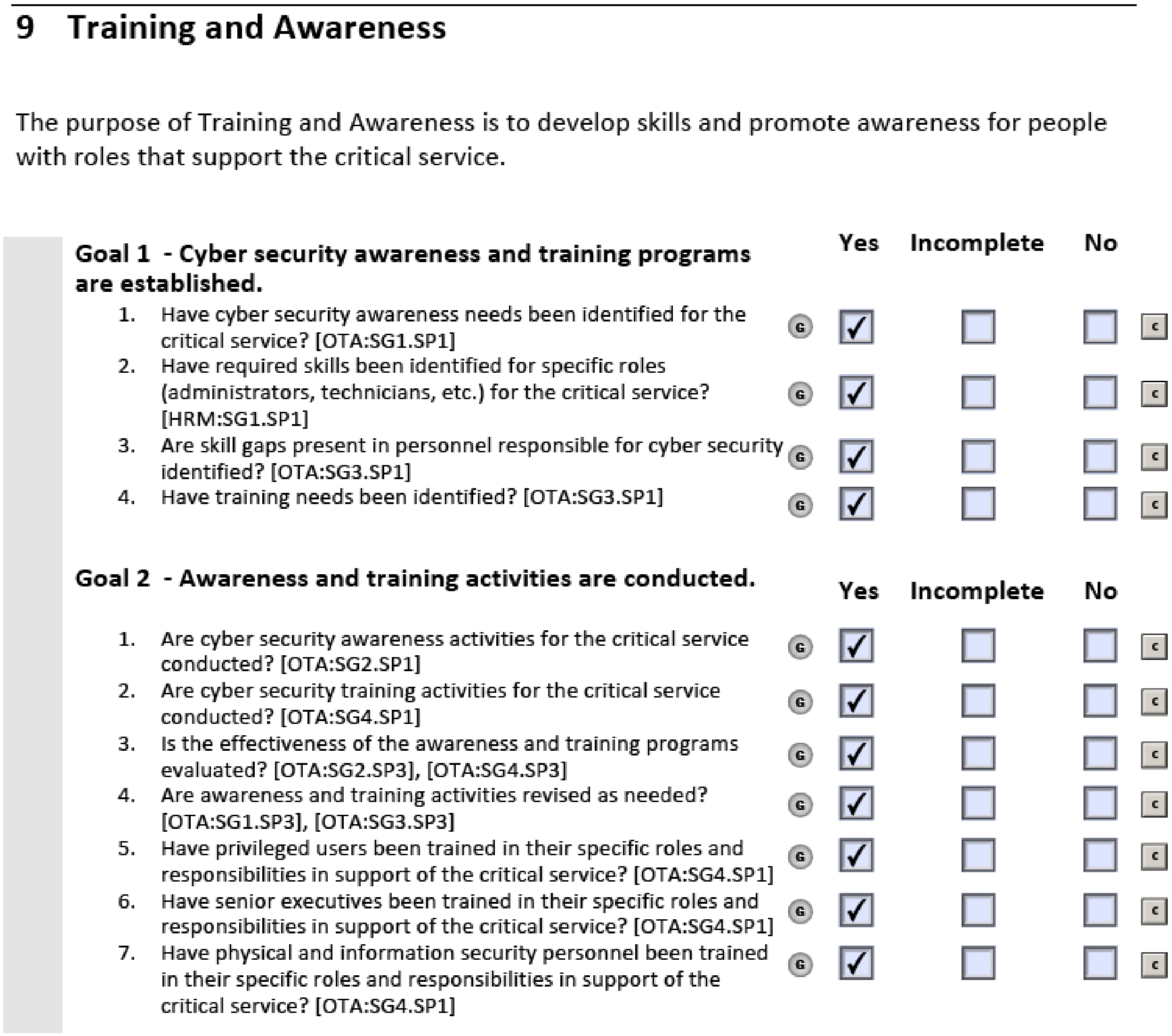
- Periodically reviewed with higher-level management (Is higher-level management aware of any issues related to the performance of the practice?).

MIL5 Defined

Indicates that all Practices in a Domain are performed, planned, managed, monitored, controlled, and consistent across all internal constituencies who have a vested interest in the performance of the practice. A defined process/practice ensures that the organization reaps the benefits of consistent performance of the practice across organizational units and that all organizational units can benefit from improvements realized in any organizational unit. At MIL5, a process/practice:

- Is defined by the organization and tailored by organizational units for their use (Is there an organization-sponsored definition of the practice from which organizational units can derive practices that fit their unique operating circumstances?).
- Is supported by improvement information that is collected by and shared among organizational units for the overall benefit of the organization (Are practice improvements documented and shared across internal constituencies so that the whole organization reaps benefits from these improvements?).

ASSESSMENT

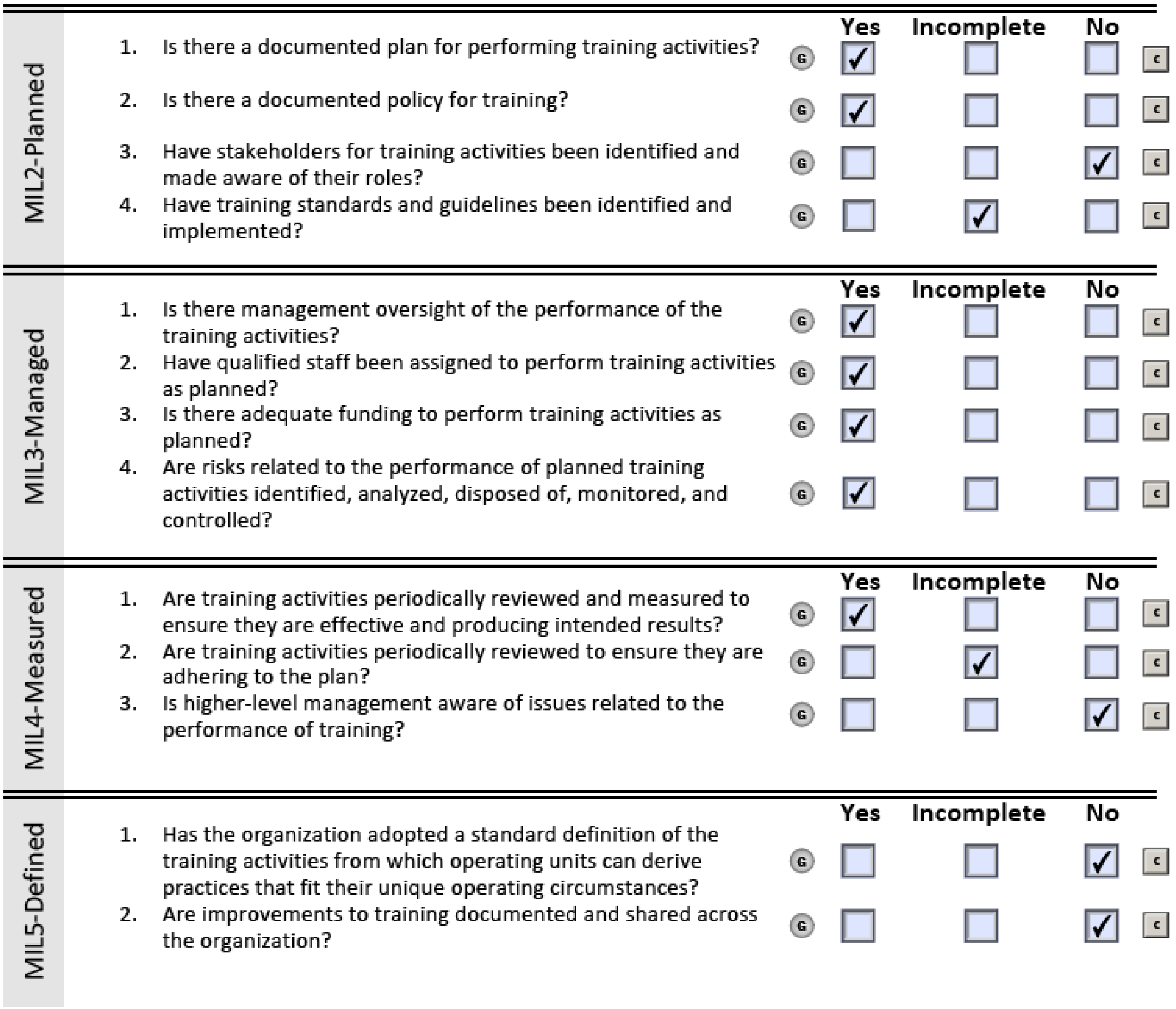


9 Training and Awareness

The purpose of Training and Awareness is to develop skills and promote awareness for people with roles that support the critical service.

Goal 1 - Cyber security awareness and training programs are established.		**Yes**	**Incomplete**	**No**	
1. Have cyber security awareness needs been identified for the critical service? [OTA:SG1.SP1]	G	☑	□	□	C
2. Have required skills been identified for specific roles (administrators, technicians, etc.) for the critical service? [HRM:SG1.SP1]	G	☑	□	□	C
3. Are skill gaps present in personnel responsible for cyber security identified? [OTA:SG3.SP1]	G	☑	□	□	C
4. Have training needs been identified? [OTA:SG3.SP1]	G	☑	□	□	C

Goal 2 - Awareness and training activities are conducted.		**Yes**	**Incomplete**	**No**	
1. Are cyber security awareness activities for the critical service conducted? [OTA:SG2.SP1]	G	☑	□	□	C
2. Are cyber security training activities for the critical service conducted? [OTA:SG4.SP1]	G	☑	□	□	C
3. Is the effectiveness of the awareness and training programs evaluated? [OTA:SG2.SP3], [OTA:SG4.SP3]	G	☑	□	□	C
4. Are awareness and training activities revised as needed? [OTA:SG1.SP3], [OTA:SG3.SP3]	G	☑	□	□	C
5. Have privileged users been trained in their specific roles and responsibilities in support of the critical service? [OTA:SG4.SP1]	G	☑	□	□	C
6. Have senior executives been trained in their specific roles and responsibilities in support of the critical service? [OTA:SG4.SP1]	G	☑	□	□	C
7. Have physical and information security personnel been trained in their specific roles and responsibilities in support of the critical service? [OTA:SG4.SP1]	G	☑	□	□	C



				Yes	Incomplete	No	
MIL2-Planned	1.	Is there a documented plan for performing training activities?	G	☑	□	□	c
	2.	Is there a documented policy for training?	G	☑	□	□	c
	3.	Have stakeholders for training activities been identified and made aware of their roles?	G	□	□	☑	c
	4.	Have training standards and guidelines been identified and implemented?	G	□	☑	□	c

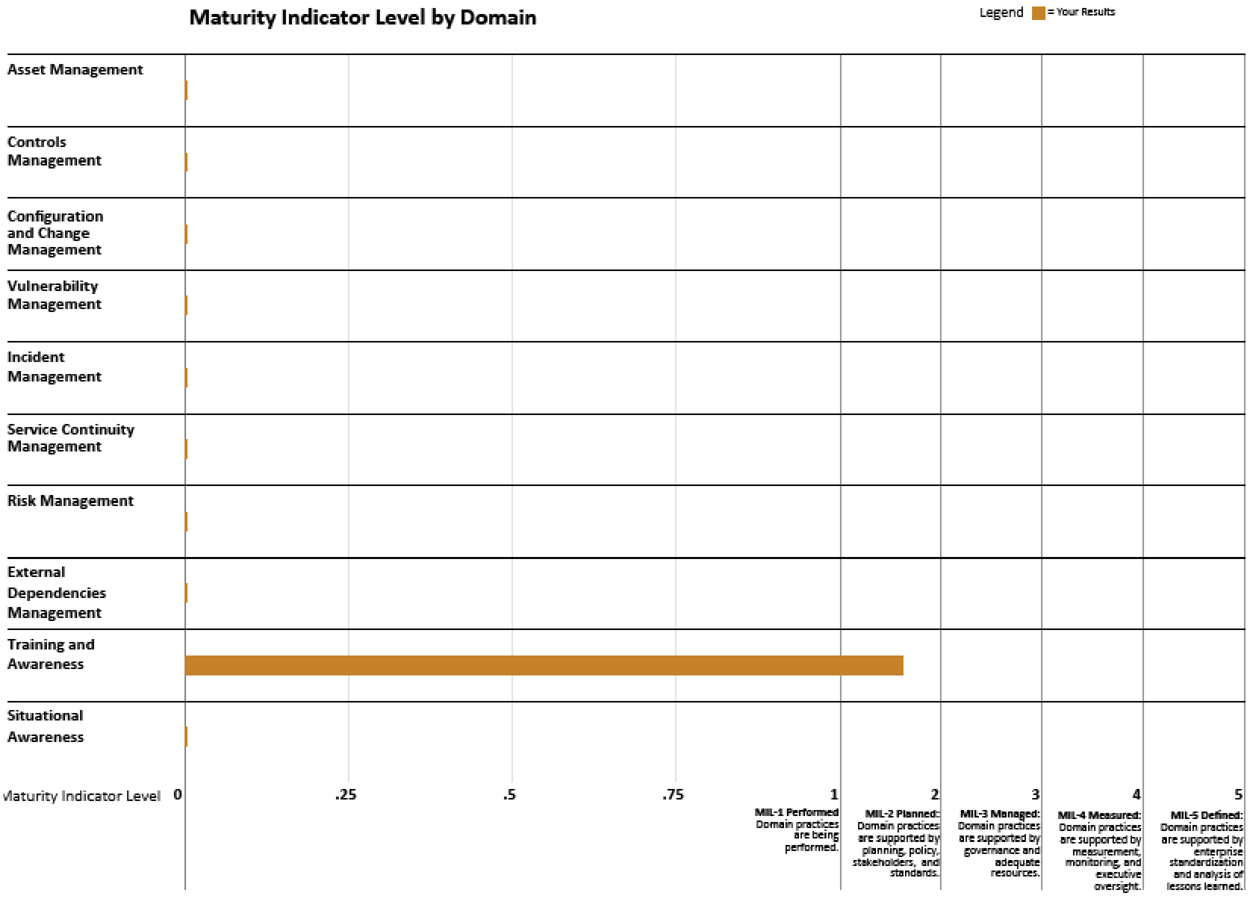
				Yes	Incomplete	No	
MIL3-Managed	1.	Is there management oversight of the performance of the training activities?	G	☑	□	□	c
	2.	Have qualified staff been assigned to perform training activities as planned?	G	☑	□	□	c
	3.	Is there adequate funding to perform training activities as planned?	G	☑	□	□	c
	4.	Are risks related to the performance of planned training activities identified, analyzed, disposed of, monitored, and controlled?	G	☑	□	□	c

				Yes	Incomplete	No	
MIL4-Measured	1.	Are training activities periodically reviewed and measured to ensure they are effective and producing intended results?	G	☑	□	□	c
	2.	Are training activities periodically reviewed to ensure they are adhering to the plan?	G	□	☑	□	c
	3.	Is higher-level management aware of issues related to the performance of training?	G	□	□	☑	c

				Yes	Incomplete	No	
MIL5-Defined	1.	Has the organization adopted a standard definition of the training activities from which operating units can derive practices that fit their unique operating circumstances?	G	□	□	☑	c
	2.	Are improvements to training documented and shared across the organization?	G	□	□	☑	c

RESULTS

Summary of CRR Results



13 | CRR Self-Assessment V 8.0.0

APPENDIX B. CENTER FOR INTERNET SECURITY CONTROLS TO THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY MAPPING

INVENTORY AND CONTROL OF HARDWARE ASSETS

Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.

Table 2. Center for Internet Security control 1.

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
1	1.1	Devices	Identify	Utilize an Active Discovery Tool	Utilize an active discovery tool to identify devices connected to the organization's network and update the hardware asset inventory.	DE.CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed.
1	1.2	Devices	Identify	Use a Passive Asset Discovery Tool	Utilize a passive discovery tool to identify devices connected to the organization's network and automatically update the organization's hardware asset inventory.	DE.CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed.
1	1.3	Devices	Identify	Use DHCP Logging to Update Asset Inventory	Use Dynamic Host Configuration Protocol (DHCP) logging on all DHCP servers or IP address management tools to update the organization's hardware asset inventory.	DE.CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed.
1	1.4	Devices	Identify	Maintain Detailed Asset Inventory	Maintain an accurate and up-to-date inventory of all technology assets with the potential to store or process information. This inventory shall include all hardware assets, whether connected to the organization's network or not.	ID.AM-1	Physical devices and systems within the organization are inventoried
						PR.DS-3	Assets are formally managed throughout removal, transfers, and disposition.

Table 2. Center for Internet Security control 1 (continuation).

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
1	1.5	Devices	Identify	Maintain Asset Inventory Information	Ensure that the hardware asset inventory records the network address, hardware address, machine name, data asset owner, and department for each asset and whether the hardware asset has been approved to connect to the network.	PR.DS-3	Assets are formally managed throughout removal, transfers, and disposition.
1	1.6	Devices	Respond	Address Unauthorized Assets	Ensure that unauthorized assets are either removed from the network, quarantined or the inventory is updated in a timely manner.	PR.DS-3	Assets are formally managed throughout removal, transfers, and disposition.
1	1.7	Devices	Protect	Deploy Port Level Access Control	Utilize port level access control, following 802.1x standards, to control which devices can authenticate to the network. The authentication system shall be tied into the hardware asset inventory data to ensure only authorized devices can connect to the network.	PR.AC-1	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes.
1	1.8	Devices	Protect	Utilize Client Certificates to Authenticate Hardware Assets	Use client certificates to authenticate hardware assets connecting to the organization's trusted network.	PR.AC-6	Identities are proofed and bound to credentials and asserted in interactions.

INVENTORY AND CONTROL OF SOFTWARE ASSETS

Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.

Table 3. Center for Internet Security control 2.

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
2	2.1	Applications	Identify	Maintain Inventory of Authorized Software	Maintain an up-to-date list of all authorized software that is required in the enterprise for any business purpose on any business system.	ID.AM-2	Software platforms and applications within the organization are inventoried.
2	2.2	Applications	Identify	Ensure Software is Supported by Vendor	Ensure that only software applications or operating systems currently supported by the software's vendor are added to the organization's authorized software inventory. Unsupported software should be tagged as unsupported in the inventory system.	ID.AM-2	Software platforms and applications within the organization are inventoried.
2	2.3	Applications	Identify	Utilize Software Inventory Tools	Utilize software inventory tools throughout the organization to automate the documentation of all software on business systems.	DE.CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed.
2	2.4	Applications	Identify	Track Software Inventory Information	The software inventory system should track the name, version, publisher, and install date for all software, including operating systems authorized by the organization.	ID.AM-2	Software platforms and applications within the organization are inventoried.

Table 3. Center for Internet Security control 2 (continuation).

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
2	2.5	Applications	Identify	Integrate Software and Hardware Asset Inventories	The software inventory system should be tied into the hardware asset inventory so all devices and associated software are tracked from a single location.	ID.AM-1	Physical devices and systems within the organization are inventoried.
						ID.AM-2	Software platforms and applications within the organization are inventoried.
2	2.6	Applications	Respond	Address unapproved software	Ensure that unauthorized software is either removed or the inventory is updated in a timely manner	DE.CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed.
2	2.7	Applications	Protect	Utilize Application Whitelisting	Utilize application whitelisting technology on all assets to ensure that only authorized software executes and all unauthorized software is blocked from executing on assets.	PR.DS-6	Integrity checking mechanisms are used to verify software, firmware, and information integrity.
						DE.CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed.
2	2.8	Applications	Protect	Implement Application Whitelisting of Libraries	The organization's application whitelisting software must ensure that only authorized software libraries (such as *.dll, *.ocx, *.so, etc.) are allowed to load into a system process.	PR.DS-6	Integrity checking mechanisms are used to verify software, firmware, and information integrity.
						DE.CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed.

Table 3. Center for Internet Security control 2 (continuation).

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
2	2.9	Applications	Protect	Implement Application Whitelisting of Scripts	The organization's application whitelisting software must ensure that only authorized, digitally signed scripts (such as *.ps1, *.py, macros, etc.) are allowed to run on a system.	PR.DS-6	Integrity checking mechanisms are used to verify software, firmware, and information integrity.
						DE.CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed.
2	2.10	Applications	Protect	Physically or Logically Segregate High Risk Applications	Physically or logically segregated systems should be used to isolate and run software that is required for business operations but incur higher risk for the organization.		

CONTINUOUS VULNERABILITY MANAGEMENT

Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.

Table 4. Center for Internet Security control 3.

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
3	3.1	Applications	Detect	Run Automated Vulnerability Scanning Tools	Utilize an up-to-date Security Content Automation Protocol (SCAP)-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.	ID.RA-1	Asset vulnerabilities are identified and documented.
						DE.CM-8	Vulnerability scans are performed.
3	3.2	Applications	Detect	Perform Authenticated Vulnerability Scanning	Perform authenticated vulnerability scanning with agents running locally on each system or with remote scanners that are configured with elevated rights on the system being tested.	DE.CM-8	Vulnerability scans are performed.
3	3.3	Users	Protect	Protect Dedicated Assessment Accounts	Use a dedicated account for authenticated vulnerability scans, which should not be used for any other administrative activities and should be tied to specific machines at specific IP addresses.		
3	3.4	Applications	Protect	Deploy Automated Operating System Patch Management Tools	Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.		

Table 4. Center for Internet Security control 3 (continuation).

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
3	3.5	Applications	Protect	Deploy Automated Software Patch Management Tools	Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor.		
3	3.6	Applications	Respond	Compare Back-to-back Vulnerability Scans	Regularly compare the results from back-to-back vulnerability scans to verify that vulnerabilities have been remediated in a timely manner.		
3	3.7	Applications	Respond	Utilize a Risk-rating Process	Utilize a risk-rating process to prioritize the remediation of discovered vulnerabilities.	RS.MI-3	Newly identified vulnerabilities are mitigated or documented as accepted risks.
						ID.RA-5	Threats, vulnerabilities, likelihoods, and impacts are used to determine risk.
						PR.IP-12	A vulnerability management plan is developed and implemented.

CONTROLLED USE OF ADMINISTRATIVE PRIVILEGES

The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.

Table 5. Center for Internet Security control 4.

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
4	4.1	Users	Detect	Maintain Inventory of Administrative Accounts	Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.	PR.AC-1	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes.
4	4.2	Users	Protect	Change Default Passwords	Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts.	PR.AC-1	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes.
4	4.3	Users	Protect	Ensure the Use of Dedicated Administrative Accounts	Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.	PR.AC-4	Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.
4	4.4	Users	Protect	Use Unique Passwords	Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		

Table 5. Center for Internet Security control 4 (continuation).

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
4	4.5	Users	Protect	Use Multifactor Authentication for All Administrative Access	Use multi-factor authentication and encrypted channels for all administrative account access.	PR.AC-7	Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks).
4	4.6	Users	Protect	Use of Dedicated Machines for All Administrative Tasks	Ensure administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. This machine will be segmented from the organization's primary network and not be allowed Internet access. This machine will not be used for reading e-mail, composing documents, or browsing the Internet.		
4	4.7	Users	Protect	Limit Access to Script Tools	Limit access to scripting tools (such as Microsoft PowerShell and Python) to only administrative or development users with the need to access those capabilities.	PR.PT-3	The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.
4	4.8	Users	Detect	Log and Alert on Changes to Administrative Group Membership	Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.	DE.CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed.
4	4.9	Users	Detect	Log and Alert on Unsuccessful Administrative Account Login	Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account.	DE.CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed.

SECURE CONFIGURATION FOR HARDWARE AND SOFTWARE ON MOBILE DEVICES, LAPTOPS, WORKSTATIONS, AND SERVERS

Establish, implement, and actively manage (track, report on, correct) the security configuration of mobile devices, laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

Table 6. Center for Internet Security control 5.

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
5	5.1	Applications	Protect	Establish Secure Configurations	Maintain documented, standard security configuration standards for all authorized operating systems and software.	PR.IP-1	A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g., concept of least functionality).
5	5.2	Applications	Protect	Maintain Secure Images	Maintain secure images or templates for all systems in the enterprise based on the organization's approved configuration standards. Any new system deployment or existing system that becomes compromised should be imaged using one of those images or templates.	PR.IP-1	A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g., concept of least functionality).
5	5.3	Applications	Protect	Securely Store Master Images	Store the master images and templates on securely configured servers, validated with integrity monitoring tools, to ensure that only authorized changes to the images are possible.	PR.IP-1	A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g., concept of least functionality).

Table 6. Center for Internet Security control 5 (continuation).

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
5	5.4	Applications	Protect	Deploy System Configuration Management Tools	Deploy system configuration management tools that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals.		
5	5.5	Applications	Detect	Implement Automated Configuration Monitoring Systems	Utilize a Security Content Automation Protocol (SCAP)-compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.	DE.CM-8	Vulnerability scans are performed.

MAINTENANCE, MONITORING, AND ANALYSIS OF AUDIT LOGS

Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.

Table 7. Center for Internet Security control 6.

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
6	6.1	Network	Detect	Utilize Three Synchronized Time Sources	Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.		
6	6.2	Network	Detect	Activate audit logging	Ensure that local logging has been enabled on all systems and networking devices.	PR.PT-1	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy.
						DE.AE-3	Event data are collected and correlated from multiple sources and sensors.
6	6.3	Network	Detect	Enable Detailed Logging	Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.	PR.PT-1	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy.
6	6.4	Network	Detect	Ensure adequate storage for logs	Ensure that all systems that store logs have adequate storage space for the logs generated.	PR.DS-4	Adequate capacity to ensure availability is maintained.

Table 7. Center for Internet Security control 6 (continuation).

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
6	6.5	Network	Detect	Central Log Management	Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.	PR.PT-1	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy.
						DE.AE-3	Event data are collected and correlated from multiple sources and sensors.
6	6.6	Network	Detect	Deploy SIEM or Log Analytic tool	Deploy Security Information and Event Management (SIEM) or log analytic tool for log correlation and analysis.	DE.AE-3	Event data are collected and correlated from multiple sources and sensors.
6	6.7	Network	Detect	Regularly Review Logs	On a regular basis, review logs to identify anomalies or abnormal events.	DE.AE-3	Event data are collected and correlated from multiple sources and sensors.
						PR.PT-1	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy.
						RS.AN-1	Notifications from detection systems are investigated.
						DE.AE-2	Detected events are analyzed to understand attack targets and methods.
6	6.8	Network	Detect	Regularly Tune SIEM	On a regular basis, tune your SIEM system to better identify actionable events and decrease event noise.	DE.AE-5	Incident alert thresholds are established.

EMAIL AND WEB BROWSER PROTECTIONS

Minimize the attack surface and the opportunities for attackers to manipulate human behavior though their interaction with web browsers and email systems.

Table 8. Center for Internet Security control 7.

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
7	7.1	Applications	Protect	Ensure Use of Only Fully Supported Browsers and Email Clients	Ensure that only fully supported web browsers and email clients are allowed to execute in the organization, ideally only using the latest version of the browsers and email clients provided by the vendor.	PR.IP-1	A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g., concept of least functionality).
7	7.2	Applications	Protect	Disable Unnecessary or Unauthorized Browser or Email Client Plugins	Uninstall or disable any unauthorized browser or email client plugins or add-on applications.	PR.IP-1	A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g., concept of least functionality).
7	7.3	Applications	Protect	Limit Use of Scripting Languages in Web Browsers and Email Clients	Ensure that only authorized scripting languages are able to run in all web browsers and email clients.	PR.IP-1	A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g., concept of least functionality).

Table 8. Center for Internet Security control 7 (continuation).

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
7	7.4	Network	Protect	Maintain and Enforce Network-Based URL Filters	Enforce network-based URL filters that limit a system's ability to connect to websites not approved by the organization. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.	DE.CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed.
7	7.5	Network	Protect	Subscribe to URL-Categorization Service	Subscribe to URL categorization services to ensure that they are up to date with the most recent website category definitions available. Uncategorized sites shall be blocked by default.	DE.CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed.
7	7.6	Network	Detect	Log all URL requester	Log all URL requests from each of the organization's systems, whether on-site or a mobile device, in order to identify potentially malicious activity and assist incident handlers with identifying potentially compromised systems.	DE.AE-3	Event data are aggregated and correlated from multiple sources and sensors.
7	7.7	Network	Protect	Use of DNS Filtering Services	Use Domain Name System (DNS) filtering services to help block access to known malicious domains.	DE.CM-1	The network is monitored to detect potential cybersecurity events.
						DE.CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed.

Table 8. Center for Internet Security control 7 (continuation).

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
7	7.8	Network	Protect	Implement DMARC and Enable Receiver-Side Verification	To lower the chance of spoofed or modified emails from valid domains, implement Domain-based Message Authentication, Reporting and Conformance (DMARC) policy and verification, starting by implementing the Sender Policy Framework (SPF) and the Domain Keys Identified Mail (DKIM) standards.	PR.IP-1	A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g., concept of least functionality).
7	7.9	Network	Protect	Block Unnecessary File Types	Block all e-mail attachments entering the organization's email gateway if the file types are unnecessary for the organization's business.	DE.CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed.
7	7.10	Network	Protect	Sandbox All Email Attachments	Use sandboxing to analyze and block inbound email attachments with malicious behavior.	DE.CM-4	Malicious code is detected.

MALWARE DEFENSES

Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action.

Table 9. Center for Internet Security control 8.

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
8	8.1	Devices	Protect	Utilize Centrally Managed Anti-Malware Software	Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.	DE.CM-4	Malicious code is detected.
8	8.2	Devices	Protect	Ensure Anti-Malware Software and Signatures are Updated	Ensure that the organization's anti-malware software updates its scanning engine and signature database on a regular basis.	DE.CM-4	Malicious code is detected.
8	8.3	Devices	Protect	Enable Operating System Anti-Exploitation Features/Deploy Anti-Exploit Technologies	Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.	PR.IP-1	A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g., concept of least functionality).
8	8.4	Devices	Detect	Configure Anti-Malware Scanning of Removable Devices	Configure devices so that they automatically conduct an anti-malware scan of removable media when inserted or connected.	DE.CM-4	Malicious code is detected.

Table 9. Center for Internet Security control 8 (continuation).

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
8	8.5	Devices	Protect	Configure Devices Not to Auto-Run Content	Configure devices to not auto-run content from removable media.	PR.PT-2	Removable media is protected and its use restricted according to policy.
8	8.6	Devices	Detect	Centralize Anti-Malware Logging	Send all malware detection events to enterprise anti-malware administration tools and event log servers for analysis and alerting.	DE.AE-3	Event data are collected and correlated from multiple sources and sensors.
8	8.7	Network	Detect	Enable DNS Query Logging	Enable DNS query logging to detect hostname lookups for known malicious domains.	DE.AE-3	Event data are collected and correlated from multiple sources and sensors.
						DE.CM-1	The network is monitored to detect potential cybersecurity events.
8	8.8	Devices	Detect	Enable Command-Line Audit Logging	Enable command-line audit logging for command shells, such as Microsoft PowerShell and Bash.	DE.AE-3	Event data are collected and correlated from multiple sources and sensors.

LIMITATION AND CONTROL OF NETWORK PORTS, PROTOCOLS, AND SERVICES

Manage (track/control/correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers

Table 10. Center for Internet Security control 9.

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
9	9.1	Devices	Identify	Associate Active Ports, Services and Protocols to Asset Inventory	Associate active ports, services and protocols to the hardware assets in the asset inventory.		
9	9.2	Devices	Protect	Ensure Only Approved Ports, Protocols and Services Are Running	Ensure that only network ports, protocols, and services listening on a system with validated business needs are running on each system.	PR.IP-1	A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g., concept of least functionality).
9	9.3	Devices	Detect	Perform Regular Automated Port Scans	Perform automated port scans on a regular basis against all systems and alert if unauthorized ports are detected on a system.	DE.CM-8	Vulnerability scans are performed.
9	9.4	Devices	Protect	Apply Host-Based Firewalls or Port Filtering	Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	PR.IP-1	A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g., concept of least functionality).
9	9.5	Devices	Protect	Implement Application Firewalls	Place application firewalls in front of any critical servers to verify and validate the traffic going to the server. Any unauthorized traffic should be blocked and logged.	PR.IP-1	A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g., concept of least functionality) systems to provide only essential capabilities.

DATA RECOVERY CAPABILITIES

The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.

Table 11. Center for Internet Security control 10.

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
10	10.1	Data	Protect	Ensure Regular Automated BackUps	Ensure that all system data is automatically backed up on a regular basis.	PR.IP-4	Backups of information are conducted, maintained, and tested.
10	10.2	Data	Protect	Perform Complete System Backups	Ensure that all of the organization's key systems are backed up as a complete system, through processes such as imaging, to enable the quick recovery of an entire system.	PR.IP-4	Backups of information are conducted, maintained, and tested.
10	10.3	Data	Protect	Test Data on Backup Media	Test data integrity on backup media on a regular basis by performing a data restoration process to ensure that the backup is properly working.	PR.DS-6	Integrity checking mechanisms are used to verify software, firmware, and information integrity.
						PR.IP-4	Backups of information are conducted, maintained, and tested.
10	10.4	Data	Protect	Ensure Protection of Backups	Ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services.	PR.DS-1	Data-at-rest is protected.
10	10.5	Data	Protect	Ensure Backups Have At least One Non-Continuously Addressable Destination	Ensure that all backups have at least one backup destination that is not continuously addressable through operating system calls.	PR.DS-1	Data-at-rest is protected.
						PR.PT-5	Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations.

SECURE CONFIGURATION FOR NETWORK DEVICES, SUCH AS FIREWALLS, ROUTERS, AND SWITCHES

Establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

Table 12. Center for Internet Security control 11.

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
11	11.1	Network	Identify	Maintain Standard Security Configurations for Network Devices	Maintain standard, documented security configuration standards for all authorized network devices.	PR.IP-1	A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g., concept of least functionality).
11	11.2	Network	Identify	Document Traffic Configuration Rules	All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.	ID.AM-3	Organizational communication and data flows are mapped.
11	11.3	Network	Detect	Use Automated Tools to Verify Standard Device Configurations and Detect Changes	Compare all network device configuration against approved security configurations defined for each network device in use and alert when any deviations are discovered.	PR.IP-3	Configuration change control processes are in place.
						DE.CM-8	Vulnerability scans are performed.

Table 12. Center for Internet Security control 11 (continuation).

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
11	11.4	Network	Protect	Install the Latest Stable Version of Any Security-Related Updates on All Network Devices	Install the latest stable version of any security-related updates on all network devices.	PR.IP-1	A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g., concept of least functionality).
11	11.5	Network	Protect	Manage Network Devices Using Multi-Factor Authentication and Encrypted Sessions	Manage all network devices using multi-factor authentication and encrypted sessions.	PR.AC-7	Users, devices, and other assets are authenticated (e.g., single-factor, multifactor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational).
11	11.6	Network	Protect	Use Dedicated Machines for All Network Administrative Tasks	Ensure network engineers use a dedicated machine for all administrative tasks or tasks requiring elevated access. This machine shall be segmented from the organization's primary network and not be allowed Internet access. This machine shall not be used for reading e-mail, composing documents, or surfing the Internet.	PR.AC-5	Network integrity is protected (e.g., network segregation, network segmentation).
11	11.7	Network	Protect	Manage Network Infrastructure Through a Dedicated Network	Manage the network infrastructure across network connections that are separated from the business use of that network, relying on separate Virtual Local Access Network (VLAN) or, preferably, on entirely different physical connectivity for management sessions for network devices.	PR.AC-5	Network integrity is protected (e.g., network segregation, network segmentation).

BOUNDARY DEFENSE

Detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data.

Table 13. Center for Internet Security control 12.

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
12	12.1	Network	Identify	Maintain an Inventory of Network Boundaries	Maintain an up-to-date inventory of all of the organization's network boundaries.	ID.AM-4	External information systems are catalogued.
12	12.2	Network	Detect	Scan for Unauthorized Connections across Trusted Network Boundaries	Perform regular scans from outside each trusted network boundary to detect any unauthorized connections which are accessible across the boundary.	ID.AM-4	External information systems are catalogued.
						DE.CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed.
12	12.3	Network	Protect	Deny Communications with Known Malicious IP Addresses	Deny communications with known malicious or unused Internet IP addresses and limit access only to trusted and necessary IP address ranges at each of the organization's network boundaries.	PR.IP-1	A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g., concept of least functionality).
12	12.4	Network	Protect	Deny Communication over Unauthorized Ports	Deny communication over unauthorized TCP or UDP ports or application traffic to ensure that only authorized protocols are allowed to cross the network boundary in or out of the network at each of the organization's network boundaries.	PR.IP-1	A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g., concept of least functionality).

Table 13. Center for Internet Security control 12 (continuation).

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
12	12.5	Network	Detect	Configure Monitoring Systems to Record Network Packets	Configure monitoring systems to record network packets passing through the boundary at each of the organization's network boundaries.	DE.CM-1	The network is monitored to detect potential cybersecurity events.
12	12.6	Network	Detect	Deploy Network-Based IDS Sensors	Deploy network-based Intrusion Detection Systems (IDS) sensors to look for unusual attack mechanisms and detect compromise of these systems at each of the organization's network boundaries.	DE.CM-1	The network is monitored to detect potential cybersecurity events.
12	12.7	Network	Protect	Deploy Network-Based Intrusion Prevention Systems	Deploy network-based Intrusion Prevention Systems (IPS) to block malicious network traffic at each of the organization's network boundaries.	DE.CM-1	The network is monitored to detect potential cybersecurity events.
12	12.8	Network	Detect	Deploy NetFlow Collection on Networking Boundary Devices	Enable the collection of NetFlow and logging data on all network boundary devices.	DE.CM-1	The network is monitored to detect potential cybersecurity events.

Table 13. Center for Internet Security control 12 (continuation).

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
12	12.9	Network	Detect	Deploy Application Layer Filtering Proxy Server	Ensure that all network traffic to or from the Internet passes through an authenticated application layer proxy that is configured to filter unauthorized connections.	DE.CM-1	The network is monitored to detect potential cybersecurity events.
						DE.CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed.
12	12.10	Network	Detect	Decrypt Network Traffic at Proxy	Decrypt all encrypted network traffic at the boundary proxy prior to analyzing the content. However, the organization may use whitelists of allowed sites that can be accessed through the proxy without decrypting the traffic.	DE.CM-1	The network is monitored to detect potential cybersecurity events
						DE.CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed.
12	12.11	Users	Protect	Require All Remote Login to Use Multi-Factor Authentication	Require all remote login access to the organization's network to encrypt data in transit and use multi-factor authentication.	PR.AC-3	Remote access is managed.
12	12.12	Devices	Protect	Manage All Devices Remotely Logging into Internal Network	Scan all enterprise devices remotely logging into the organization's network prior to accessing the network to ensure that each of the organization's security policies has been enforced in the same manner as local network devices.	PR.MA-2	Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access.
						PR.AC-3	Remote access is managed.

DATA PROTECTION

The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.

Table 14. Center for Internet Security control 13.

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
13	13.1	Data	Identify	Maintain an Inventory of Sensitive Information	Maintain an inventory of all sensitive information stored, processed, or transmitted by the organization's technology systems, including those located on-site or at a remote service provider.	ID.AM-5	Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value.
13	13.2	Data	Protect	Remove Sensitive Data or Systems Not Regularly Accessed by Organization	Remove sensitive data or systems not regularly accessed by the organization from the network. These systems shall only be used as standalone systems (disconnected from the network) by the business unit needing to occasionally use the system or completely virtualized and powered off until needed.	PR.DS-3	Assets are formally managed throughout removal, transfers, and disposition.
13	13.3	Data	Detect	Monitor and Block Unauthorized Network Traffic	Deploy an automated tool on network perimeters that monitors for unauthorized transfer of sensitive information and blocks such transfers while alerting information security professionals.	PR.DS-5	Protections against data leaks are implemented.
13	13.4	Data	Protect	Only Allow Access to Authorized Cloud Storage or Email Providers	Only allow access to authorized cloud storage or email providers.	PR.DS-5	Protections against data leaks are implemented.

Table 14. Center for Internet Security control 13 (continuation).

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
13	13.5	Data	Detect	Monitor and Detect Any Unauthorized Use of Encryption	Monitor all traffic leaving the organization and detect any unauthorized use of encryption.	DE.CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed.
13	13.6	Data	Protect	Encrypt the Hard Drive of All Mobile Devices.	Utilize approved whole disk encryption software to encrypt the hard drive of all mobile devices.	PR.DS-1	Data-at-rest is protected.
13	13.7	Data	Protect	Manage USB Devices	If USB storage devices are required, enterprise software should be used that can configure systems to allow the use of specific devices. An inventory of such devices should be maintained.	PR.PT-2	Removable media is protected and its use restricted according to policy.
13	13.8	Data	Protect	Manage System's External Removable Media's Read/Write Configurations	Configure systems not to write data to external removable media, if there is no business need for supporting such devices.	PR.PT-2	Removable media is protected and its use restricted according to policy.
13	13.9	Data	Protect	Encrypt Data on USB Storage Devices	If USB storage devices are required, all data stored on such devices must be encrypted while at rest.	PR.PT-2	Removable media is protected and its use restricted according to policy.

CONTROLLED ACCESS BASED ON THE NEED TO KNOW

The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.

Table 15. Center for Internet Security control 14.

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
14	14.1	Network	Protect	Segment the Network Based on Sensitivity	Segment the network based on the label or classification level of the information stored on the servers, locate all sensitive information on separated VLANs.	PR.AC-5	Network integrity is protected (e.g., network segregation, network segmentation).
14	14.2	Network	Protect	Enable Firewall Filtering Between VLANs	Enable firewall filtering between VLANs to ensure that only authorized systems are able to communicate with other systems necessary to fulfill their specific responsibilities.	PR.AC-5	Network integrity is protected (e.g., network segregation, network segmentation).
14	14.3	Network	Protect	Disable Workstation to Workstation Communication	Disable all workstation to workstation communication to limit an attacker's ability to move laterally and compromise neighboring systems, through technologies such as Private VLANs or micro segmentation.	PR.AC-5	Network integrity is protected (e.g., network segregation, network segmentation).
14	14.4	Data	Protect	Encrypt All Sensitive Information in Transit	Encrypt all sensitive information in transit.	PR.DS-2	Data-in-transit is protected.

Table 15. Center for Internet Security control 14 (continuation).

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
14	14.5	Data	Detect	Utilize an Active Discovery Tool to Identify Sensitive Data	Utilize an active discovery tool to identify all sensitive information stored, processed, or transmitted by the organization's technology systems, including those located on-site or at a remote service provider, and update the organization's sensitive information inventory.		
14	14.6	Data	Protect	Protect Information through Access Control Lists	Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	PR.AC-4	Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.
14	14.7	Data	Protect	Enforce Access Control to Data through Automated Tools	Use an automated tool, such as host-based Data Loss Prevention, to enforce access controls to data even when data is copied off a system.	PR.DS-5	Protections against data leaks are implemented.
14	14.8	Data	Protect	Encrypt Sensitive Information at Rest	Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.	PR.DS-1	Data-at-rest is protected.
14	14.9	Data	Detect	Enforce Detail Logging for Access or Changes to Sensitive Data	Enforce detailed audit logging for access to sensitive data or changes to sensitive data (utilizing tools such as File Integrity Monitoring or Security Information and Event Monitoring).	PR.DS-6	Integrity checking mechanisms are used to verify software, firmware, and information integrity.

WIRELESS ACCESS CONTROL

The processes and tools used to track/control/prevent/correct the security use of wireless local area networks (WLANs), access points, and wireless client systems.

Table 16. Center for Internet Security control 15.

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
15	15.1	Network	Identify	Maintain an Inventory of Authorized Wireless Access Points	Maintain an inventory of authorized wireless access points connected to the wired network.	ID.AM-3	Organizational communication and data flows are mapped.
						DE.AE-1	A baseline of network operations and expected data flows for users and systems is established and managed.
15	15.2	Network	Detect	Detect Wireless Access Points Connected to the Wired Network	Configure network vulnerability scanning tools to detect and alert on unauthorized wireless access points connected to the wired network.	DE.CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed.
15	15.3	Network	Detect	Use a Wireless Intrusion Detection System (WIDS)	Use a WIDS to detect and alert on unauthorized wireless access points connected to the network.	DE.CM-1	The network is monitored to detect potential cybersecurity events.
15	15.4	Devices	Protect	Disable Wireless Access on Devices if Not Required	Disable wireless access on devices that do not have a business purpose for wireless access.	PR.IP-1	A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g., concept of least functionality).
15	15.5	Devices	Protect	Limit Wireless Access on Client Devices	Configure wireless access on client machines that do have an essential wireless business purpose, to allow access only to authorized wireless networks and to restrict access to other wireless networks.	PR.IP-1	A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g., concept of least functionality).

Table 16. Center for Internet Security control 15 (continuation).

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
15	15.6	Devices	Protect	Disable Peer-to-Peer Wireless Network Capabilities on Wireless Clients	Disable peer-to-peer (ad hoc) wireless network capabilities on wireless clients.	PR.IP-1	A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g., concept of least functionality).
15	15.7	Network	Protect	Leverage the Advanced Encryption Standard (AES) to Encrypt Wireless Data	Leverage the Advanced Encryption Standard (AES) to encrypt wireless data in transit.	PR.DS-2	Data-in-transit is protected.
15	15.8	Network	Protect	Use Wireless Authentication Protocols that Require Mutual, Multi-Factor Authentication	Ensure that wireless networks use authentication protocols such as Extensible Authentication Protocol-Transport Layer Security (EAP/TLS), which requires mutual, multi-factor authentication.	PR.AC-7	Users, devices, and other assets are authenticated (e.g., single-factor, multifactor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks).
15	15.9	Devices	Protect	Disable Wireless Peripheral Access of Devices	Disable wireless peripheral access of devices (such as Bluetooth and NFC), unless such access is required for a business purpose.	PR.IP-1	A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g., concept of least functionality).
15	15.10	Network	Protect	Create Separate Wireless Network for Personal and Untrusted Devices	Create a separate wireless network for personal or untrusted devices. Enterprise access from this network should be treated as untrusted and filtered and audited accordingly.	PR.AC-5	Network integrity is protected (e.g., network segregation, network segmentation).

ACCOUNT MONITORING AND CONTROL

Actively manage the life cycle of system and application accounts—their creation, use, dormancy, deletion—in order to minimize opportunities for attackers to leverage them.

Table 17. Center for Internet Security control 16.

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
16	16.1	Users	Identify	Maintain an Inventory of Authentication Systems	Maintain an inventory of each of the organization's authentication systems, including those located on-site or at a remote service provider.	PR.AC-1	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes.
16	16.2	Users	Protect	Configure Centralized Point of Authentication	Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.		
16	16.3	Users	Protect	Require Multi-Factor Authentication	Require multi-factor authentication for all user accounts, on all systems, whether managed on-site or by a third-party provider.	PR.AC-7	Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks).
16	16.4	Users	Protect	Encrypt or Hash all Authentication Credentials	Encrypt or hash with a salt all authentication credentials when stored.	PR.AC-1	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes.
16	16.5	Users	Protect	Encrypt Transmittal of Username and Authentication Credentials	Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.	PR.DS-2	Data-in-transit is protected.

Table 17. Center for Internet Security control 16 (continuation).

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
16	16.6	Users	Identify	Maintain an Inventory of Accounts	Maintain an inventory of all accounts organized by authentication system.	PR.AC-1	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes.
16	16.7	Users	Protect	Establish Process for Revoking Access	Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor. Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.	PR.AC-1	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes.
						PR.IP-11	Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening).
16	16.8	Users	Respond	Disable Any Unassociated Accounts	Disable any account that cannot be associated with a business process or business owner.	PR.AC-1	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes.
16	16.9	Users	Respond	Disable Dormant Accounts	Automatically disable dormant accounts after a set period of inactivity.	PR.AC-1	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes.
16	16.10	Users	Protect	Ensure All Accounts Have an Expiration Date	Ensure that all accounts have an expiration date that is monitored and enforced.	PR.AC-1	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes.

Table 17. Center for Internet Security control 16 (continuation).

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
16	16.11	Users	Protect	Lock Workstation Sessions After Inactivity	Automatically lock workstation sessions after a standard period of inactivity.	PR.IP-1	A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g., concept of least functionality).
16	16.12	Users	Detect	Monitor Attempts to Access Deactivated Accounts	Monitor attempts to access deactivated accounts through audit logging.	DE.CM-3	Personnel activity is monitored to detect potential cybersecurity events.
16	16.13	Users	Detect	Alert on Account Login Behavior Deviation	Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.	DE.CM-3	Personnel activity is monitored to detect potential cybersecurity events.

IMPLEMENT A SECURITY AWARENESS AND TRAINING PROGRAM

For all functional roles in the organization (prioritizing those mission-critical to the business and its security), identify the specific knowledge, skills and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs.

Table 18. Center for Internet Security control 17.

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
17	17.1	N/A	N/A	Perform a Skills Gap Analysis	Perform a skills gap analysis to understand the skills and behaviors workforce members are not adhering to, using this information to build a baseline education roadmap.		
17	17.2	N/A	N/A	Deliver Training to Fill the Skills Gap	Deliver training to address the skills gap identified to positively impact workforce members' security behavior.	PR.AT-5	Physical and cybersecurity personnel understand their roles and responsibilities.
						PR.AT-4	Senior executives understand their roles and responsibilities.
						PR.AT-3	Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities.
						PR.AT-2	Privileged users understand their roles and responsibilities.
						PR.AT-1	All users are informed and trained.
17	17.3	N/A	N/A	Implement a Security Awareness Program	Create a security awareness program for all workforce members to complete on a regular basis to ensure they understand and exhibit the necessary behaviors and skills to help ensure the security of the organization. The organization's security awareness program should be communicated in a continuous and engaging manner.	PR.AT-1	All users are informed and trained.
						ID.AM-6	Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established.

Table 18. Center for Internet Security control 17 (continuation).

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
17	17.4	N/A	N/A	Update Awareness Content Frequently	Ensure that the organization's security awareness program is updated frequently (at least annually) to address new technologies, threats, standards and business requirements.		
17	17.5	N/A	N/A	Train Workforce on Secure Authentication	Train workforce members on the importance of enabling and utilizing secure authentication.	PR.AT-1	All users are informed and trained.
17	17.6	N/A	N/A	Train Workforce on Identifying Social Engineering Attacks	Train the workforce on how to identify different forms of social engineering attacks, such as phishing, phone scams and impersonation calls.	PR.AT-1	All users are informed and trained.
17	17.7	N/A	N/A	Train Workforce on Sensitive Data Handling	Train workforce on how to identify and properly store, transfer, archive and destroy sensitive information.	PR.AT-1	All users are informed and trained.
17	17.8	N/A	N/A	Train Workforce on Causes of Unintentional Data Exposure	Train workforce members to be aware of causes for unintentional data exposures, such as losing their mobile devices or emailing the wrong person due to autocomplete in email.	PR.AT-1	All users are informed and trained.
17	17.9	N/A	N/A	Train Workforce Members on Identifying and Reporting Incidents	Train employees to be able to identify the most common indicators of an incident and be able to report such an incident.	PR.AT-1	All users are informed and trained.

APPLICATION SOFTWARE SECURITY

Manage the security life cycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses.

Table 19. Center for Internet Security control 18.

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
18	18.1	N/A	N/A	Establish Secure Coding Practices	Establish secure coding practices appropriate to the programming language and development environment being used.		
18	18.2	N/A	N/A	Ensure Explicit Error Checking is Performed for All In-House Developed Software	For in-house developed software, ensure that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats.		
18	18.3	N/A	N/A	Verify That Acquired Software is Still Supported	Verify that the version of all software acquired from outside your organization is still supported by the developer or appropriately hardened based on developer security recommendations.		
18	18.4	N/A	N/A	Only Use Up to Date and Trusted Third-Party Components	Only use up-to-date and trusted third-party components for the software developed by the organization.		
18	18.5	N/A	N/A	Use Only Standardized and Extensively Reviewed Encryption Algorithms	Use only standardized and extensively reviewed encryption algorithms.	PR.DS-1	Data-at-rest is protected.
						PR.DS-2	Data-in-transit is protected.

Table 19. Center for Internet Security control 18 (continuation).

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
18	18.6	N/A	N/A	Ensure Software Development Personnel are Trained in Secure Coding	Ensure that all software development personnel receive training in how to write secure code for their specific development environment and responsibilities.		
18	18.7	N/A	N/A	Apply Static and Dynamic Code Analysis Tools	Apply static and dynamic analysis tools to verify that secure coding practices are being adhered to for internally developed software.		
18	18.8	N/A	N/A	Establish a Process to Accept and Address Reports of Software Vulnerabilities	Establish a process to accept and address reports of software vulnerabilities, including providing a means for external entities to contact your security group.	RS.AN-5	Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g., internal testing, security bulletins, or security researchers).
18	18.9	N/A	N/A	Separate Production and Non-Production Systems	Maintain separate environments for production and non-production systems. Developers should not have unmonitored access to production environments.	PR.DS-7	The development and testing environment(s) are separate from the production environment.

Table 19. Center for Internet Security control 18 (continuation).

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
18	18.10	N/A	N/A	Deploy Web Application Firewalls (WAF)	Protect web applications by deploying WAFs that inspect all traffic flowing to the web application for common web application attacks. For applications that are not web-based, specific application firewalls should be deployed if such tools are available for the given application type. If the traffic is encrypted, the device should either sit behind the encryption or be capable of decrypting the traffic prior to analysis. If neither option is appropriate, a host-based web application firewall should be deployed.		
18	18.11	N/A	N/A	Use Standard Hardening Configuration Templates for Databases	For applications that rely on a database, use standard hardening configuration templates. All systems that are part of critical business processes should also be tested.	PR.IP-1	A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g., concept of least functionality).

INCIDENT RESPONSE AND MANAGEMENT

Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.

Table 20. Center for Internet Security control 19.

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
19	19.1	N/A	N/A	Document Incident Response Procedures	Ensure that there are written incident response plans that define roles of personnel as well as phases of incident handling/management.	PR.IP-9	Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.
19	19.2	N/A	N/A	Assign Job Titles and Duties for Incident Response	Assign job titles and duties for handling computer and network incidents to specific individuals and ensure tracking and documentation throughout the incident through resolution.	PR.IP-9	Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.
						ID.GV-2	Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners.
						RS.CO-1	Personnel know their roles and order of operations when a response is needed.
						DE.DP-1	Roles and responsibilities for detection are well defined to ensure accountability.

Table 20. Center for Internet Security control 19 (continuation).

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
19	19.3	N/A	N/A	Designate Management Personnel to Support Incident Handling	Designate management personnel, as well as backups, who will support the incident handling process by acting in key decision-making roles.	PR.IP-9	Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.
						DE.DP-1	Roles and responsibilities for detection are well defined to ensure accountability.
19	19.4	N/A	N/A	Devise Organization-wide Standards for Reporting Incidents	Devise organization-wide standards for the time required for system administrators and other workforce members to report anomalous events to the incident handling team, the mechanisms for such reporting, and the kind of information that should be included in the incident notification.	RS.CO-2	Incidents are reported consistent with established criteria.
19	19.5	N/A	N/A	Maintain Contact Information for Reporting Security Incidents	Assemble and maintain information on third-party contact information to be used to report a security incident, such as Law Enforcement, relevant government departments, vendors, and Information Sharing and Analysis Centers (ISAC) partners.	ID.SC-5	Response and recovery planning and testing are conducted with suppliers and third-party providers.

Table 20. Center for Internet Security control 19 (continuation).

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
19	19.6	N/A	N/A	Publish Information Regarding Reporting Computer Anomalies and Incidents	Publish information for all workforce members, regarding reporting computer anomalies and incidents to the incident handling team. Such information should be included in routine employee awareness activities.	DE.DP-4	Event detection information is communicated.
						RS.CO-4	Coordination with stakeholders occurs consistent with response plans.
19	19.7	N/A	N/A	Conduct Periodic Incident Scenario Sessions for Personnel	Plan and conduct routine incident, response exercises and scenarios for the workforce involved in the incident response to maintain awareness and comfort in responding to real world threats. Exercises should test communication channels, decision making, and incident responders technical capabilities using tools and data available to them.	PR.IP-10	Response and recovery plans are tested.
19	19.8	N/A	N/A	Create Incident Scoring and Prioritization Schema	Create incident scoring and prioritization schema based on known or potential impact to your organization. Utilize score to define frequency of status updates and escalation procedures.	RS.AN-4	Incidents are categorized consistent with response plans.

PENETRATION TESTS AND RED TEAM EXERCISES

Test the overall strength of an organization's defense (the technology, the processes, and the people) by simulating the objectives and actions of an attacker.

Table 21. Center for Internet Security control 20.

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
20	20.1	N/A	N/A	Establish a Penetration Testing Program	Establish a program for penetration tests that includes a full scope of blended attacks, such as wireless, client-based, and web application attacks.		
20	20.2	N/A	N/A	Conduct Regular External and Internal Penetration Tests	Conduct regular external and internal penetration tests to identify vulnerabilities and attack vectors that can be used to exploit enterprise systems successfully.		
20	20.3	N/A	N/A	Perform Periodic Red Team Exercises	Perform periodic Red Team exercises to test organizational readiness to identify and stop attacks or to respond quickly and effectively.		
20	20.4	N/A	N/A	Include Tests for Presence of Unprotected System Information and Artifacts	Include tests for the presence of unprotected system information and artifacts that would be useful to attackers, including network diagrams, configuration files, older penetration test reports, e-mails or documents containing passwords or other information critical to system operation.		

Table 21. Center for Internet Security control 20 (continuation).

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	NIST CSF	Subcategory Name
20	20.5	N/A	N/A	Create Test Bed for Elements Not Typically Tested in Production	Create a test bed that mimics a production environment for specific penetration tests and Red Team attacks against elements that are not typically tested in production, such as attacks against supervisory control and data acquisition and other control systems.		
20	20.6	N/A	N/A	Use Vulnerability Scanning and Penetration Testing Tools in Concert	Use vulnerability scanning and penetration testing tools in concert. The results of vulnerability scanning assessments should be used as a starting point to guide and focus penetration testing efforts.		
20	20.7	N/A	N/A	Ensure Results from Penetration Test are Documented Using Open, Machine-readable Standards	Wherever possible, ensure that Red Team results are documented using open, machine-readable standards (e.g., SCAP). Devise a scoring method for determining the results of Red Team exercises so that results can be compared over time.		
20	20.8	N/A	N/A	Control and Monitor Accounts Associated with Penetration Testing	Any user or system accounts used to perform penetration testing should be controlled and monitored to make sure they are only being used for legitimate purposes, and are removed or restored to normal function after testing is over.	PR.AC-1	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes.

APPENDIX C: REFERENCES

Center for Internet Security (CIS), "CIS Controls V7.1 Mapping to NIST CSF." Retrieved from: https://www.cisecurity.org/white-papers/cis-controls-v7-1-mapping-to-nist-csf/

Center for Internet Security (CIS), "CIS Controls Version 7.1," 2019. Retrieved from: https://www.cisecurity.org/controls/

Department of Homeland Security (DHS), "Critical Infrastructure Sectors," 2013. Retrieved from: https://www.dhs.gov/cisa/critical-infrastructure-sectors

Department of Homeland Security (DHS), "Cyber Resilience Review (CRR): NIST Cybersecurity Framework Crosswalks," 2016. Retrieved from: https://www.us-cert.gov/sites/default/files/c3vp/csc-crr-nist-framework-crosswalk.pdf

Department of Homeland Security (DHS), "Cyber Security Procurement Language for Control Systems," 2009. Retrieved from: https://ics-cert.us-cert.gov/sites/default/files/documents/Procurement_Language_Rev4_100809_S508C.pdf

NIST, "FIPS 199 Standards for Security Categorization of Federal Information and Information Systems," 2004. Retrieved from: https://csrc.nist.gov/publications/detail/fips/199/final

NIST, "Risk Management Framework for Information Systems and Organizations," October 2018. Retrieved from: https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/archive/2017-09-28

NIST, "SP 800-37 Rev. 2 Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach," 2018. Retrieved from: https://csrc.nist.gov/publications/detail/sp/800-37/rev-1/final

NIST, "SP 800-53 Rev. 4 Security and Privacy Controls for Federal Information Systems and Organizations," 2015. Retrieved from: https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final

NIST, "SP 800-53A Rev. 4 Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans," 2014. Retrieved from: https://csrc.nist.gov/publications/detail/sp/800-53a/rev-4/final

NIST, "SP 800-82 Rev. 2 Guide to Industrial Control Systems (ICS) Security," 2015. Retrieved from: https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final

NIST, "SP 800-144 Guidelines on Security and Privacy in Public Cloud Computing," 2011. Retrieved from: https://csrc.nist.gov/publications/detail/sp/800-144/final

Steven VanRoekel, Executive Office of the President "Security Authorization of Information Systems in Cloud Computing Environments Memorandum," 2011. Retrieved from: https://www.fedramp.gov/assets/resources/documents/FedRAMP_Policy_Memo.pdf

TWiki, "NIST Cloud Computing Collaboration Site." Retrieved from: https://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/CloudSecurity

Wiki, "List of TCP and UDP port numbers." Retrieved from: https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

U.S. Department of Transportation
Federal Highway Administration
Office of Operations
1200 New Jersey Avenue, SE
Washington, DC 20590

https://ops.fhwa.dot.gov

September 2019
FHWA-HOP-19-059