

Intelligent Transportation Systems (ITS) Security Control Set for Dynamic Message Signs

www.its.dot.gov/index.htm

Final Report – April 2026
FHWA-JPO-26-004



U.S. Department of Transportation

Produced by Leidos
U.S. Department of Transportation
Office of the Assistant Secretary for Research and Technology

Notice

This document is disseminated under the sponsorship of the Department of Transportation in the interest of information exchange. The United States Government assumes no liability for its contents or use thereof.

The U.S. Government is not endorsing any manufacturers, products, or services cited herein and any trade name that may appear in the work has been included only because it is essential to the contents of the work.

Technical Report Documentation Page

1. Report No. FHWA-JPO-26-004	2. Government Accession No.	3. Recipient's Catalog No.	
4. Title and Subtitle Intelligent Transportation Systems (ITS) Security Control Set for Dynamic Message Sign		5. Report Date April 2026	
		6. Performing Organization Code	
7. Author(s) Brian Russell, Elijah Pichler, Reilly Fastring, Robert Sanchez (ORCID: 0000-0002-0763-6146)		8. Performing Organization Report No.	
9. Performing Organization Name and Address Leidos Inc. 1750 Presidents Street Reston, VA 20190		10. Work Unit No. (TRAIS)	
		11. Contract or Grant No. 693JJ322A000005	
12. Sponsoring Agency Name and Address Federal Highway Administration 1200 New Jersey Avenue, SE Washington, DC 20590		13. Type of Report and Period Covered Final Report, October 2024 – July 2026	
		14. Sponsoring Agency Code ITS JPO	
15. Supplementary Notes The Task Order Contracting Officer Representative for this project was Joe Gregory.			
16. Abstract This control set document identifies security controls typically needed to mitigate security risks to dynamic message signs (DMS) operating in the role of intelligent transportation systems roadway equipment described by the Traffic Information Dissemination service package in the Architecture Reference for Cooperative and Intelligent Transportation (ARC-IT) TM06. The objective of this control set is to provide a means to better protect DMS and the information flows supported by its interfaces as more advanced features are added. The controls (primarily technical controls) relevant to DMS are specified in this control set document. Security controls are safeguards or countermeasures prescribed for a system or an organization to protect the confidentiality, integrity, and availability of the system and its information.			
17. Keywords Intelligent Transportation Systems, Cybersecurity, Control Sets, NIST SP 800-53		18. Distribution Statement No restrictions. This document is available to the public through the National Technical Information Service, Springfield, VA 22161. http://www.ntis.gov	
19. Security Classif. (of this report) unclassified	20. Security Classif. (of this page) unclassified	21. No. of Pages 233	22. Price N/A

Table of Contents

Chapter 1. Identification.....	1
Purpose, Scope, and Applicability	1
Revisions	2
Sources	2
Relationship between ARC-IT, the Cybersecurity Framework, and Control Sets.....	3
Chapter 2. Physical Object Characteristics.....	5
Definition/Description	5
Physical Object Device Security Class by Service Package	7
Assumptions and Characteristics.....	9
Resources for Identifying Threats, Vulnerabilities, and Predisposing Conditions	10
Connection between the ITS Profile, CSF Subfunctions, and NIST SP 800-53 Controls	11
Chapter 3. Summary of Control Specifications	13
Chapter 4. Detailed Control Specifications	30
AC Family – Access Control.....	31
AT Family – Awareness and Training.....	50
AU Family – Audit and Accountability.....	51
CA Family – Assessment, Authorization, and Monitoring.....	59
CM Family – Configuration Management.....	63
CP Family – Contingency Planning	70
IA Family – Identification and Authentication	71
IR Family – Incident Response	78
MA Family – Maintenance.....	80
PE Family – Physical and Environmental Protection	83
PL Family – Planning	87
PM Family – Program Management.....	88
RA Family – Risk Assessment.....	90
SA Family – System and Services Acquisition	93
SC Family – System and Communications Protection	99
SI Family – System and Information Integrity	115
SR Family – Supply Chain Risk Management.....	123

Chapter 5. Implementation Considerations	127
CM-5, Access Restrictions for Change.....	127
PE-3, Physical Access Control.....	127
SI-4(14), System Monitoring Wireless Intrusion Detection	127
Appendix A. Threats, Vulnerabilities, and Predisposing Conditions.....	129
Appendix B. NIST SP 800-53 Security Control's Mapping.....	147
Appendix C. Abbreviations.....	199
Appendix D. Control Family Abbreviations.....	201
Appendix E. Glossary	203
References.....	207

List of Tables

Table 1. Physical Object Device Security Class by DMS	8
Table 2. Control Specifications for DMS	14
Table 3. Adversarial Threat Events	129
Table 4. Non-Adversarial Threat Events	136
Table 5. Physical Object Threat Events	137
Table 6. Vulnerabilities and Predisposing Conditions	138
Table 7. Mapping of DMS Mission Objectives to NIST CSF Subcategories and NIST SP 800-53 Controls	147

List of Figures

Figure 1. Illustration. Primary DMS Application Components and Related Systems/Users	6
Figure 2. Diagram. Reference Architecture for a DMS System with the Scope of the DMS Model SE Documents.....	7
Figure 3. Diagram. DMS Connectivity and Component Structure	10

Chapter 1. Identification

Purpose, Scope, and Applicability

This control set document defines the security and privacy controls necessary to address risks specific to dynamic message signs (DMS) within intelligent transportation systems (ITS). Derived from National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53,⁽¹⁾ these controls focus on safeguarding the confidentiality, integrity, and availability (C-I-A) of DMS assets and their supported information flows. As DMS technology evolves to include advanced features, this control set aims to mitigate risks inherent to DMS operations and interfaces, enabling robust, secure data dissemination. Designed for use by system owners, managers, integrators, engineers, and manufacturers, this control set offers a structured approach to identifying security requirements for DMS.

The controls outlined here, primarily technical in nature, are intended to complement broader ITS security measures. They include necessary organizational controls from NIST SP 800-53⁽¹⁾ that are relevant to the design, implementation, and operational support of DMS. Additionally, these controls help address residual risks from overarching ITS infrastructures that may impact DMS, helping to protect against unauthorized access, data manipulation, and service disruptions. By referencing the larger security posture of ITS systems, DMS stakeholders can identify gaps and apply controls specific to DMS to mitigate unaddressed risks. This proactive approach ensures that critical non-technical controls essential to DMS security are integrated, whether by manufacturers, infrastructure operators, or organizational stakeholders, to maintain secure, resilient ITS environments. The controls (primarily technical controls) relevant to DMS are specified in this control set document. Security controls are safeguards or countermeasures prescribed for a system operator or an organization to protect the C-I-A of the system and its information. This control set is intended to be used by system and service managers/owners, system integrators, system engineers, and system component manufacturers to derive security requirements for DMS.

The risk mitigation and protection provided by other controls implemented in larger systems, operations, or data centers, or by the infrastructure owner/operators (IOOs)¹ operating ITS, provide benefit to physical objects that are part of these larger systems, centers, or IOOs. Owners, operators, and users of DMS may examine the security assessment of the larger system to determine which risks might not be mitigated and/or might be passed on to DMS itself and then select controls that mitigate that risk. Some controls tagged in NIST SP 800-53,⁽¹⁾ as organizational controls are included in this control set because aspects of the control need to be conveyed to the manufacturer/vendor for design and implementation. In some cases, the organizational control is purely non-technical but it is important to successfully securing the DMS that the control cannot be ignored and are addressed by the IOO before, during, or after a DMS is delivered and installed.

¹ NIST refers generically to “the organization.” This document refers specifically to the IOO, which includes public agencies.

The scope of this control set focuses primarily on how a typical DMS system would be implemented by the ITS community for common use cases using today's technology. The effort is to identify and select controls applicable to most DMS implementations. Nuances of other implementations (e.g., legacy or future systems) may be addressed in the guidance element of individual controls in "Detailed Control Specifications" Chapter 4 of this control set.

Revisions

This control set document should be evaluated for revision, when necessary, including when:

- NIST issues new revisions of NIST SP 800-30, *Guide for Conducting Risk Assessments*.⁽³⁵⁾
- NIST issues new revisions of NIST SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*.⁽¹⁾
- NIST issues new revisions of NIST SP 800-82, *Guide to Industrial Control Systems (ICS) Security*.⁽⁷⁾
- NIST issues new revisions of The Cybersecurity Framework (CSF).⁽⁷⁾
- Architecture Reference for Cooperative and Intelligent Transportation (ARC-IT)⁽¹⁸⁾ is significantly revised in areas that affect DMS.
- Relevant standards are developed or updated.
- Significant changes to technologies are made.
- New threats and/or vulnerabilities are discovered that affect the subject of this document.
- New methodologies for assessing threats and/or vulnerabilities are developed.
- National Transportation Communications for ITS Protocol (NTCIP) issues new revisions of NTCIP 1203v03, *Object Definitions for Dynamic Message Signs (DMS)*.⁽⁵⁾
- The Federal Highway Administration (FHWA) makes significant changes to *Model Systems Engineering Documents for Dynamic Message Sign (DMS) Systems*, version 1.0.⁽⁶⁾

Sources

The following are key resources used to create this document and inform the identification of controls needed to mitigate risk to DMS. Each resource includes a brief context for how it influenced or informed the controls selection.

- ARC-IT version 9.3, for device security classes based on the potential impact to the C-I-A of information flows between physical objects and their associated functional objects.⁽¹⁸⁾
- NIST SP 800-30 Revision 1, for typical threat sources and vulnerabilities that may be relevant or tailored to ITS.⁽³⁵⁾
- NIST SP 800-82 Revision 3, *Guide to Operational Technology (OT) Security*, for operational technology (was industrial control system) threats and vulnerabilities that may be relevant or tailored to ITS.⁽³⁾

- MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) version 17.1, for ICS for threat sources' tactics, techniques, and procedures and mitigations that may also be relevant or tailored to ITS.⁽³⁴⁾
- MITRE ATT&CK version 17.1, for enterprise for threat sources' tactics, techniques, and procedures and mitigations that may also be relevant or tailored to ITS.⁽³⁴⁾
- NTCIP 1203 version 3, *Object Definitions for Dynamic Message Signs (DMS)*, for overall object definition and industry standards for DMS communication.⁽⁵⁾
- ITS Cybersecurity Framework Profile 2.0 (ITS Profile) for prioritizing subcategories mapped to security controls, which can be used to guide control specifications in this control set.⁽⁴⁾
- *USDOT FHWA Model Systems Engineering Documents for Dynamic Message Sign (DMS) Systems*, version 1.0, for system requirements and physical/operational environment specific to DMS.⁽⁶⁾
- *Model Systems Engineering Document—ITS Application: Dynamic Message Signs*, for common use cases of DMS to better understand unique vulnerabilities and threats to DMS systems.⁽⁶⁾

Relationship between ARC-IT, the Cybersecurity Framework, and Control Sets

The ITS Profile was used to inform the control selections in this document. The ITS Profile identifies and prioritizes ITS mission objectives, which a given system with its physical devices may support. The ITS Profile also aligns functions, categories, and subcategories in the cybersecurity framework core with those mission objectives. Controls that support higher-priority subcategories must be considered for inclusion at each of the five device security class levels in ARC-IT.⁽¹⁸⁾ Final control selections are also guided by the physical object owning/operating organization's risk tolerances and may be justified after cost/benefit analyses, as it is not feasible or affordable to mitigate all risks.

ARC-IT was used as the source for defining and characterizing systems, devices, device security classes, physical objects, functional objects, information flows, and service packages relevant to ITS. ARC-IT provides a common framework for planning, defining, and integrating ITS deployments. As a reference architecture, ARC-IT provides a common basis for planners and engineers to conceive and develop ITS projects. This is accomplished by presenting four views:

- **Enterprise View** considers ITS from an organizational perspective. It identifies stakeholder organizations or enterprise objects—the people and organizations who plan, develop, operate, maintain, and use ITS. It defines stakeholder roles and the relationships between stakeholders. This is also the view where needs are defined since ARC-IT, and more broadly ITS, is driven by the needs of stakeholder organizations, their constituents, and customers.
- **Functional View** looks at ITS from a functional perspective. Functional requirements are defined that support ITS user needs. Processes and data flows provide a structured presentation of functions and interactions that support the requirement
- **Physical View** defines the physical objects (the systems and devices) that provide ITS functionality. Information flows define the flow of information between physical objects. Functional objects organize the functionality that is required to support ITS within each physical object.

- **Communications View** defines how physical objects communicate. It defines communications standards and profiles that are combined into communications solutions that specify how information can be reliably and securely shared between physical objects.

Within ARC-IT, these views are presented in service packages, which include the subset of ARC-IT that meets one or more user needs. A service package will include some number of physical objects. Each physical object may contain one or more functional objects defining ITS-specific functionality necessary to address those user needs. The physical objects are connected by information flows that can be implemented by the defined communications solutions. ARC-IT v9.3 has 152 service packages organized into 12 functional areas.⁽¹⁸⁾

Cybersecurity in ARC-IT⁽¹⁸⁾ is addressed through the analysis of the C-I-A required for information flows within each service package. Each information flow was scored using a low-moderate-high (L-M-H) rating. These ratings are then applied to the physical object where the information flow originates or ends, and a device security class is assigned to those objects. Because there could be 27 possible (and potentially untenable) combinations of L-M-H ratings over the C-I-A dimensions, ARC-IT groups the ratings into five device security classes.⁽¹⁸⁾ Planners and engineers should select devices that are certified to meet the requirements for a class but could avoid the unnecessary expense of using devices that meet higher classes than necessary for an application.

Only the controls (primarily technical controls²) relevant to the DMS are specified in this control set document. This approach is necessary to simplify and decrease the size of the document and to make the document more manageable and usable. The risk mitigation and protection provided by other controls implemented in larger systems, operations or data centers, or by the organizations operating ITS provide benefit to physical objects that are part of these larger systems, centers, or organizations. Control assessments of physical objects will be limited in scope, but owners, operators, and users of DMS may examine the security and privacy assessment results to determine the acceptability of the physical objects for use in a larger system, and the assessment reports may be incorporated into the larger system's risk management process and documentation.

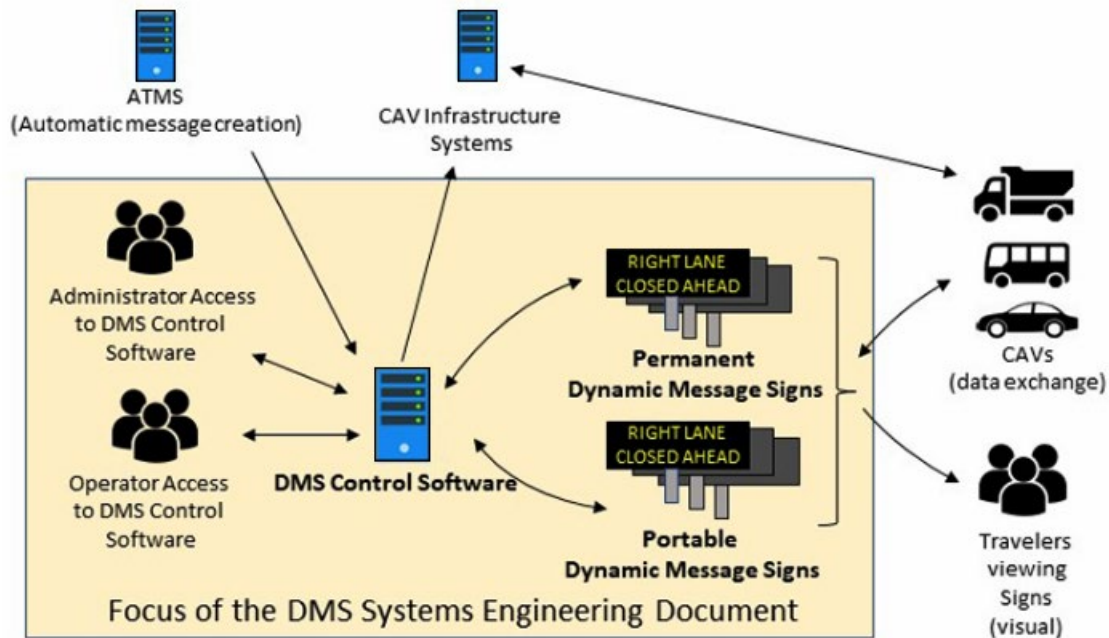
² The technical controls are typically implemented by systems rather than by people.

Chapter 2. Physical Object Characteristics

Definition/Description

DMS, also referred to as variable message sign or changeable message sign in some States, operates in the field environment,³ as described in ARC-IT, typically as part of the implementation of ITS roadway equipment for real-time driver information. DMS operate under centralized control from traffic management centers (TMC), using protocols like NTCIP for interoperability. The primary components of a DMS, according to *ITS Application: Dynamic Message Signs*,⁽⁵⁾ are represented and illustrated in Figure 1. If additional components, such as sensors or communication interfaces, are integrated into the DMS setup, it may be necessary to address any increased security risks posed by these components by adjusting the control selections accordingly.

³ ARC-IT defines the field as: Infrastructure proximate to the transportation network which performs surveillance (e.g., traffic detectors, cameras), traffic control (e.g., signal controllers), information provision (e.g., DMS), connected vehicle processing and communications (e.g., roadside units), and local transaction (e.g., tolling, parking) functions and are typically governed by IOO centralized or cloud-based transportation management systems.

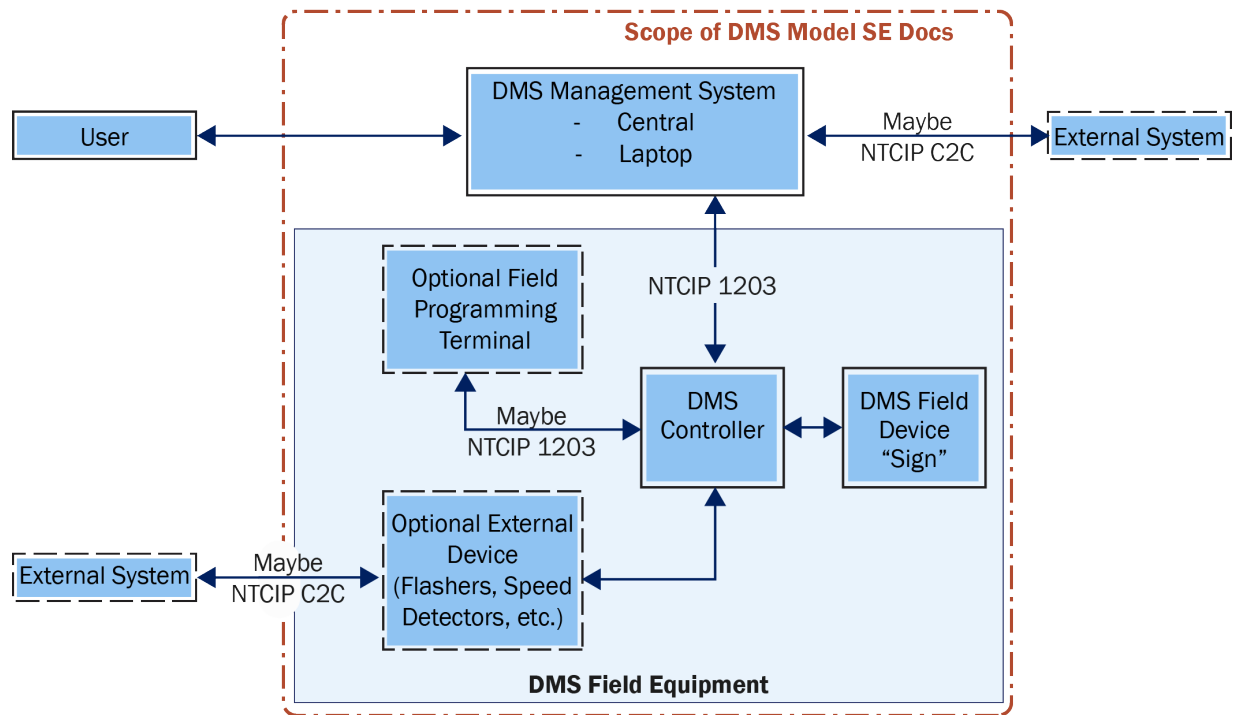


Source: MnDOT Model Systems Engineering Document ITS Applications: DMS, 2019

Figure 1. Illustration. Primary DMS Application Components and Related Systems/Users

The DMS operates in outdoor environments, typically mounted along highways, arterial roads, or other major transportation routes. The device is exposed to varying weather conditions, physical wear, and potential security risks, which necessitate robust physical and cybersecurity protections. The types and quality of connectivity and interfaces required by this DMS include secure, low-latency communication with the central traffic management system (TMS), typically via encrypted Transmission Control Protocol/Internet Protocol (TCP/IP) or wireless networks. Local interfaces, such as Ethernet or serial connections, may be used for maintenance and diagnostic purposes.

Additionally, the DMS may be integrated into broader ITS, such as advanced traffic management systems (ATMS), emergency management systems, and dynamic traffic control applications, enhancing road safety, traffic flow, and incident response. In most cases the primary DMS system is enclosed in a protective housing and connected to the main sign controller either wirelessly or through a communication line. In addition to the physical signs deployed in the field, DMS applications typically include additional components that facilitate communication between the central computer, maintenance computer, and the sign controller. The reference architecture, found in *Model Systems Engineering Documents for Dynamic Message Sign (DMS) Systems*,⁽⁶⁾ is shown in figure 2.



Source: FHWA, *Model Systems Engineering Documents for Dynamic Message Sign (DMS) Systems*, 2018.

Figure 2. Diagram. Reference Architecture for a DMS System with the Scope of the DMS Model SE Documents

The connectivity must support both real-time message updates and system monitoring. The information flows for this physical object include real-time data exchanges between the DMS and the central TMS, with message updates, system status, and diagnostic data being exchanged bidirectionally. According to ARC-IT, these information flows are defined as follows: roadway dynamic signage status, which pertains to the current operating status of DMS; roadway dynamic signage data, which includes information used to initialize, configure, and control DMS; and dynamic sign coordination, which involves the direct flow of information between field equipment, including the initialization, configuration, and control of DMS. These flows ensure that traffic updates are accurate and timely while enabling the monitoring of system functionality for performance and security.

The scope of this control set relevant to the DMS includes ensuring the C-I-A of DMS operations within ITS environments. This involves securing data flows, maintaining system functionality, and ensuring the reliability of message delivery in real-time scenarios. The functions of this physical object include displaying dynamic messages such as road conditions, incident alerts, travel times, and other critical information to drivers, including connected and automated vehicles (CAVs). These messages are updated in real-time through data exchanges with a central TMS.

Physical Object Device Security Class by Service Package

Table 1 conveys that DMS appears in 24 service packages. This table also indicates the device security class (1–5) for each physical object based on its application within a specific service package. Users of

this control set document should examine this table to identify the device security class for the physical object, then go to Table 2 to determine which controls are necessary to protect that physical object as part of the service package.

Given a DMS may be used within multiple service packages, it is necessary to consider the impact of the DMS on the mission/functions the service package supports, which is addressed by aligning control specifications under the appropriate device security class in Table 2.

Table 1. Physical Object Device Security Class by DMS

Service Package	Device Security Class
	DMS
CVO05: Commercial Vehicle Parking	2
MC03: Roadway Automated Treatment	2
MC06: Work Zone Management	2
MC12: One-Way Convoy Driving	2
PM04: Regional Parking Management	2
PS10: Wide-Area Alert	2
PT10: Intermittent Bus Lanes	2
PT12: Transit Vehicle at Station/Stop Warnings	2
ST03: Eco-Traffic Metering	2
ST07: Eco-Lanes Management	2
ST10: Low Emissions Zone Management	2
TI07: In-Vehicle Signage	2
TM05: Traffic Metering	2
TM06: Traffic Information Dissemination	2
TM17: Speed Warning and Enforcement	2
TM18: Drawbridge Management	2
TM19: Roadway Closure Management	2
TM20: Variable Speed Limits	2
TM21: Speed Harmonization	2

Service Package	Device Security Class
	DMS
TM22: Dynamic Lane Management and Shoulder Use	2
TM24: Tunnel Management	2
TM25: Wrong Way Vehicle Detection and Warning	2
VS09: Reduced Speed Zone Warning / Lane Closure	2
VS10: Restricted Lane Warnings	2

CVO = Commercial Vehicle Operations; DM = Data Management; MC = Maintenance and Construction; PM = Parking Management; PS = Public Safety; PT = Public Transportation; ST = Sustainable Travel; TI = Traveler Information and Personal Mobility; TM = Traffic Management; VS = Vehicle Safety.

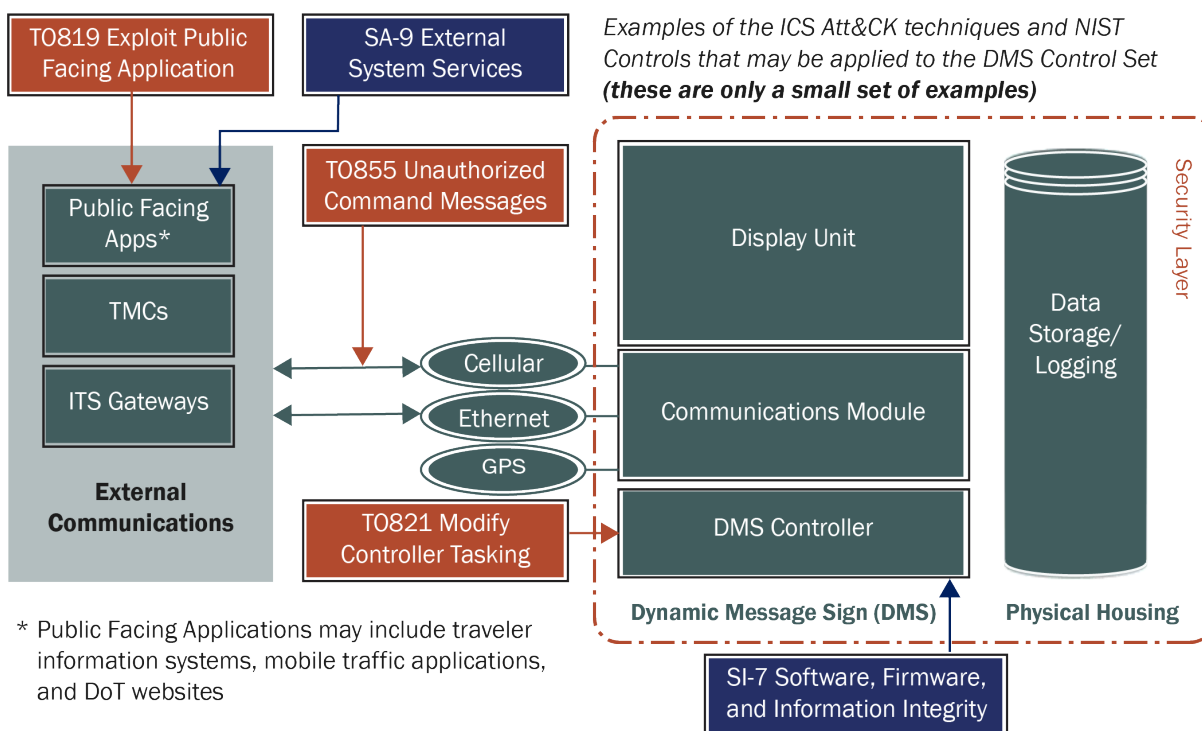
Assumptions and Characteristics

This control set document is necessary because ITS physical objects have a set of characteristics and assumptions that often differentiate them from other types of technologies (e.g., general enterprise information technology). Figure 3 illustrates the connectivity and component structure of DMS devices, providing insight into the rationale behind the selected assumptions. Those assumptions are listed here and are discussed in the following paragraphs.

- Assumption #1: DMS devices are connected to a secure network or supports ethernet connection.
 - The DMS devices are assumed to be connected to a secure network, either through cellular, wireless fidelity (Wi-Fi), or a hardwired Ethernet connection. As shown in Figure 3, DMS devices are assumed to be capable of securely connecting to multiple external services, including public-facing applications, TMC, and other ITS gateways. Devices operating in isolated or offline modes may require alternative controls not covered in this set.
- Assumption #2: DMS systems are connected to a reliable power source for continuous power and very limited downtime.
 - DMS systems are assumed to have access to a stable and reliable power source, such as grid electricity or backup generators, to ensure continuous operation with minimal interruptions. The controls in this document, such as PE-11(1): Emergency Power — Minimal Operational Capability, address emergency backup power (e.g., uninterruptible power supply) rather than baseline power supply. Agencies with limited power infrastructure may need additional controls to mitigate risks of downtime due to baseline power disruptions.
- Assumption #3: The DMS is securely linked to the sign controller, either through a wired or wireless connection. If the sign controller is housed locally in a roadside cabinet, it is safeguarded against physical tampering.
 - The DMS is assumed to maintain a secure connection to its sign controller, whether through wired or wireless means, with measures in place to prevent unauthorized access

or data interception. For controllers housed in roadside cabinets, physical security features, such as tamper-resistant locks or enclosures, are assumed to be implemented.

- Assumption #4: DMS utilizes secure network protocols
 - The control set assumes that DMS devices use secure and standardized communication protocols, such as NTCIP 1203⁽⁵⁾ over Hypertext Transfer Protocol Secure, Simple Network Management Protocol (SNMPv3), and secure File Transfer Protocol (FTP). This ensures data integrity, confidentiality, and availability during transmission. Devices that rely on legacy or insecure protocols are excluded from this control set, as they are more vulnerable to cyberattacks, including eavesdropping, spoofing, and data manipulation.



Source: TrustThink, 2024

Figure 3. Diagram. DMS Connectivity and Component Structure

Resources for Identifying Threats, Vulnerabilities, and Predisposing Conditions

A broad set of adversarial and non-adversarial threat events that could potentially impact DMS is provided in Appendix A. Threats, Vulnerabilities, and Predisposing Conditions containing Table 3 (adversarial) and Table 4 (non-adversarial). The properties of DMS may also present unique opportunities to a threat source, specifically addressing how the threat source can manipulate the process of DMS or the supported service package to cause physical damage. Table 5, in Appendix A. Threats, Vulnerabilities, and Predisposing Conditions, provides an overview of potential threat events more specific to DMS. Table 6 contains any vulnerabilities and predisposing conditions that may impact DMS systems given the uniqueness of the system.

Threat events listed in Appendix A. Threats, Vulnerabilities, and Predisposing Conditions focus on the DMS, not the larger system comprised of various types of physical objects and other components. Various threat events may ultimately impact DMS or its mission/operations, either by compromise of the DMS itself or the larger system (e.g., control center). In the case of potential compromise of the larger system, that larger system (not the physical object) must implement certain protections to mitigate those risks. Only if the DMS can implement a protection measure to mitigate the risk will the threat be considered relevant to the DMS itself and, therefore, controls will be selected in this document to mitigate only those risks.

Connection between the ITS Profile, CSF Subfunctions, and NIST SP 800-53 Controls

To establish alignment with the selected NIST SP 800-53⁽¹⁾ controls detailed in Chapter 3 and the ITS CSF Profile,⁽⁷⁾ a comprehensive table was developed to map relevant mission objectives for the DMS system to NIST CSF subcategories, as presented in Table 7. These mission objectives were defined based on the DMS system's physical and technical attributes, such as its real-time messaging capabilities and digital display features. The following mission objectives were chosen for the DMS system: #1: Improve physical safety of the transportation ecosystem, #2: Increase the efficiency of the transportation ecosystem, #3: Collect, manage, use, and disseminate data, #8: Build privacy protections into ITS operations, and #11 Enhance telecommunications and networking to facilitate emerging ITS capabilities.

Table 7 lists all high-priority NIST CSF subcategories corresponding to these mission objectives, along with carefully selected moderate-priority subcategories relevant to the DMS system. Using the NIST CSF informative reference tool, appropriate NIST SP 800-53⁽¹⁾ controls were identified to address the DMS system's specific vulnerabilities. For high-priority subcategories, all recommended controls from the NIST reference tool were included. A justification will be provided if any high-priority related security controls are not selected in the Notes column in Table 7. For moderate-priority subcategories, only the most relevant security controls were selected. The controls in Table 7 represent a focused subset, with additional controls determined through risk assessments tailored to the DMS system's unique attributes.

Chapter 3. Summary of Control Specifications

Table 2 summarizes each of the controls listed in “Detailed Control Specifications” in Chapter 4. Each control is assigned symbols indicating specific attributes, as defined below, and is categorized according to the device security classes specified in ARC-IT. For more intricate security controls, not all device security classes will be assigned to implement them. In such cases, the symbol “NS” is used to indicate non-applicability. The controls and enhancements were selected to secure the DMS system, considering its technical and physical properties. Responsibilities for implementing each control are assigned to designated parties, such as manufacturers, IOO, or both.

Table 2 contains a summary of the control specifications as they apply in this control set document. The symbols used in the table are as follows:

- “NS” indicates the control is not selected.
- “G” indicates there is guidance for the control, including specific applicability guidance or possibly implementation tailoring guidance.
- “V” indicates this control set document defines a value for an ITS-specific parameter for the control,⁴ but only to address unique physical object risks and to direct the developer to comply; other parameter values are left to the discretion of the ITS program that is deploying the physical objects to set based on industry practices.
- “R” indicates there is at least one risk reference or resource that informs the control selection
- “S” indicates there is a standard or practice that the control helps to meet.
- “M” indicates the control is implemented by the manufacturer of the physical object.
- “I” indicates the control is implemented by the IOO organization.
- “M/I” indicates the control is implemented by the manufacturer and the IOO organization.

Due to the nature of physical objects and the operational environment, implementation of selected controls may need to deviate from implementations for typical information systems, as is described in the Discussion element⁵ for each control in NIST SP 800-53.⁽¹⁾ Unique implementations are described in the guidance provided in “Detailed Control Specifications” of this control set document. The last column of Table 2 below indicates if the control should be implemented by the DMS manufacturer or by the IOO organization. Allocation of responsibility for the controls may be different than what is implied in the

⁴ The control text in NIST SP 800-53 may include a parameter (e.g., password length and complexity) that needs to be defined before the control can be implemented.

⁵ The Discussion element was previously called Supplemental Guidance in NIST SP 800-53 Revision table 5.

control text in NIST SP 800-53,⁽¹⁾ in that the device itself may need to implement controls typically implemented by the organization, or vice versa.

Table 2. Control Specifications for DMS

ID	Title	Device Security Class					Responsibility (Manufacturer (M); IOO (I))
		1	2	3	4	5	
AC-1	Policy and Procedures	GVR	GVR	GVR	GVR	GVR	I
AC-2	Account Management	GVR	GVR	GVR	GVR	GVR	I
AC-2(3)	Disable Accounts	GVRs	GVRs	GVRs	GVRs	GVRs	M/I
AC-2(4)	Automated Audit Actions	NS	G	G	G	G	I
AC-2(5)	Inactivity Logout	GVRs	GVRs	GVRs	GVRs	GVRs	M/I
AC-3	Access Enforcement	GR	GR	GR	GR	GR	M/I
AC-3(2)	Dual Authorization	NS	GV	GV	GV	GV	I
AC-3(4)	Access Enforcement Discretionary Access Control	NS	NS	G	G	G	M/I
AC-4	Information Flow Enforcement	GVR	GVR	GVR	GVR	GVR	M/I
AC-4(4)	Flow Control of Encrypted Information	GV	GV	GV	GV	GV	M/I
AC-5	Separation of Duties	NS	NS	GVR	GVR	GVR	M/I
AC-6	Least Privilege	GR	GR	GR	GR	GR	I
AC-6(1)	Authorize Access to Security Functions	GVR	GVR	GVR	GVR	GVR	M/I
AC-6(3)	Network Access to Privileged Commands	NS	GVR	GVR	GVR	GVR	I
AC-6(8)	Privilege Levels for Code Execution	NS	GV	GV	GV	GV	M/I

ID	Title	Device Security Class					Responsibility (Manufacturer (M); IOO (I))
		1	2	3	4	5	
AC-6(10)	Prohibit Non-Privileged Users from Executing Privileged Functions	GR	GR	GR	GR	GR	M/I
AC-7	Unsuccessful Logon Attempts	GVR	GVR	GVR	GVR	GVR	M/I
AC-8	System Use Notification	NS	GVR	GVR	GVR	GVR	M/I
AC-9	Previous Logon Notification	NS	NS	GR	GR	GR	I
AC-10	Concurrent Session Control	NS	NS	GVR	GVR	GVR	M/I
AC-11	Device Lock	NS	NS	GVR	GVR	GVR	M/I
AC-12	Session Termination	NS	GVR	GVR	GVR	GVR	M/I
AC-12(1)	User-Initiated Logouts	NS	GV	GV	GV	GV	M
AC-14	Permitted Actions without Identification or Authentication	GV	GV	GV	GV	GV	M/I
AC-16	Security and Privacy Attributes	GVS	GVS	GVS	GVS	GVS	M/I
AC-17	Remote Access	GR	GR	GR	GR	GR	M/I
AC-17(1)	Monitoring and Control	NS	GR	GR	GR	GR	M/I
AC-17(2)	Protection of Confidentiality and Integrity Using Encryption	GRS	GRS	GRS	GRS	GRS	M
AC-18	Wireless Access	GR	GR	GR	GR	GR	I
AC-18(1)	Authentication and Encryption	GVRs	GVRs	GVRs	GVRs	GVRs	M

ID	Title	Device Security Class					Responsibility (Manufacturer (M); IOO (I))
		1	2	3	4	5	
AC-18(3)	Disable Wireless Networking	NS	NS	G	G	G	M/I
AC-18(5)	Antennas and Transmission Power Levels	NS	NS	NS	GR	GR	I
AC-20	Use of External Systems	NS	GVRs	GVRs	GVRs	GVRs	M/I
AC-20(1)	Limits on Authorized Use	NS	NS	G	G	G	I
AC-20(2)	Portable Storage Devices – Restricted Use	NS	NS	GVS	GVS	GVS	I
AC-21	Information Sharing	NS	GVR	GVR	GVR	GVR	I
AC-24	Access Control Decisions	NS	GV	GV	GV	GV	M/I
AT-03	Role-Based Training	GVR	GVR	GVR	GVR	GVR	M/I
AU-2	Event Logging	GVRs	GVRs	GVRs	GVRs	GVRs	M/I
AU-3	Content of Audit Records	G	G	G	G	G	M/I
AU-4	Audit Log Storage Capacity	NS	GVR	GVR	GVR	GVR	M/I
AU-4(1)	Transfer to Alternate Storage	NS	NS	NS	GVR	GVR	M/I
AU-5	Response to Audit Processing Failures	GV	GV	GV	GV	GV	M/I
AU-5(1)	Storage Capacity Warning	GV	GV	GV	GV	GV	M/I
AU-5(2)	Real-Time Alerts	NS	NS	GVR	GVR	GVR	M/I
AU-6	Audit Record Review, Analysis, and Reporting	GVR	GVR	GVR	GVR	GVR	I

ID	Title	Device Security Class					Responsibility
		1	2	3	4	5	
AU-6(4)	Central Review and Analysis	G	G	G	G	G	I
AU-6(6)	Correlation with Physical Monitoring	NS	NS	G	G	G	M/I
AU-7	Audit Record Reduction and Report Generation	NS	NS	G	G	G	M
AU-9	Protection of Audit Information	NS	NS	GVR	GVR	GVR	M/I
AU-9(2)	Store on Separate Physical Systems or Components	NS	NS	GVR	GVR	GVR	M/I
AU-9(3)	Cryptographic Protection	NS	NS	NS	GRS	GRS	M
AU-11	Audit Record Retention	NS	GV	GV	GV	GV	I
AU-12	Audit Record Generation	GVR	GVR	GVR	GVR	GVR	M
AU-12(3)	Changes by Authorized Individuals	GVR	GVR	GVR	GVR	GVR	M
AU-13	Monitoring for Information Disclosure	NS	NS	GV	GV	GV	I
AU-14	Session Audit	NS	GV	GV	GV	GV	M
AU-16	Cross-Organizational Audit Logging	NS	GVS	GVS	GVS	GVS	M
CA-3	Information Exchange	GNS	GVR	GVR	GVR	GVR	I
CA-3(6)	Transfer Authorizations	NS	G	G	G	G	I
CA-3(7)	Transitive Information Exchanges	NS	G	G	G	G	I

ID	Title	Device Security Class					Responsibility (Manufacturer (M); IOO (I))
		1	2	3	4	5	
CA-5	Plan of Action and Milestones	GVR	GVR	GVR	GVR	GVR	I
CA-6	Authorization	GV	GV	GV	GV	GV	I
CA-7	Continuous Monitoring	NS	GVR	GVR	GVR	GVR	I
CA-7(6)	Automation Support for Monitoring	NS	NS	NS	GV	GV	M/I
CA-8	Penetration Testing	GVRs	GVRs	GVRs	GVRs	GVRs	I
CA-9	Internal System Connections	GVR	GVR	GVR	GVR	GVR	I
CM-2	Baseline Configuration	GVS	GVS	GVS	GVS	GVS	M/I
CM-3	Configuration Change Control	GR	GR	GR	GR	GR	M/I
CM-4	Impact Analysis	NS	NS	GR	GR	GR	I
CM-5	Access Restrictions for Change	GR	GR	GR	GR	GR	I
CM-5(4)	Dual Authorization	NS	G	G	G	G	I
CM-6	Configuration Settings	GV	GV	GV	GV	GV	M/I
CM-7	Least Functionality	GVRs	GVRs	GVRs	GVRs	GVRs	M/I
CM-7(2)	Prevent Program Execution	GV	GV	GV	GV	GV	M/I
CM-7(4)	Unauthorized Software – Deny by Exception	GV	GV	GV	GV	GV	M/I
CM-7(5)	Authorized Software – Allow by Exception	GV	GV	GV	GV	GV	M/I

ID	Title	Device Security Class					Responsibility (Manufacturer (M); IOO (I))
		1	2	3	4	5	
CM-7(9)	Prohibiting the Use of Unauthorized Hardware	GV	GV	GV	GV	GV	M/I
CM-8	System Component Inventory	GV	GV	GV	GV	GV	I
CM-8(1)	Updates During Installation and Removal	G	G	G	G	G	I
CM-9	Configuration Management Plan	GV	GV	GV	GV	GV	I
CM-10	Software Usage Restrictions	G	G	G	G	G	I
CM-11	User-Installed Software	GV	GV	GV	GV	GV	M/I
CM-11(2)	Software Installation with Privileged Status	G	G	G	G	G	M/I
CP-9	System Backup	NS	GVR	GVR	GVR	GVR	M/I
CP-9(1)	Testing for Reliability and Integrity	NS	GVR	GVR	GVR	GVR	M/I
CP-10	System Recovery and Reconstitution	NS	NS	GVR	GVR	GVR	M/I
IA-2	Identification and Authentication (Organizational Users)	GR	GR	GR	GR	GR	M/I
IA-2(1)	Multifactor Authentication to Privileged Accounts	GR	GR	GR	GR	GR	I
IA-2(2)	Multifactor Authentication to Non-Privileged Accounts	NS	NS	NS	GR	GR	I

ID	Title	Device Security Class					Responsibility (Manufacturer (M); IOO (I))
		1	2	3	4	5	
IA-3	Device Identification and Authentication	GVR	GVR	GVR	GVR	GVR	M/I
IA-5	Authenticator Management	GVRs	GVRs	GVRs	GVRs	GVRs	M/I
IA-5(1)	Password-Based Authentication	GVRs	GVRs	GVRs	GVRs	GVRs	M/I
IA-5(2)	Public Key-Based Authentication	NS	NS	GRS	GRS	GRS	M/I
IA-6	Authenticator Feedback	GR	GR	GR	GR	GR	M
IA-7	Cryptographic Module Authentication	NS	NS	GRS	GRS	GRS	M
IA-8	Identification and Authentication (Non-Organizational Users)	GR	GR	GR	GR	GR	M
IA-9	Service Identification and Authentication	GVR	GVR	GVR	GVR	GVR	M/I
IA-11	Re-authentication	GV	GV	GV	GV	GV	M
IR-2	Incident Response Training	NS	GV	GV	GV	GV	I
IR-3	Incident Response Testing	NS	GV	GV	GV	GV	I
IR-4	Incident Handling	NS	GR	GR	GR	GR	I
IR-5	Incident Monitoring	NS	GR	GR	GR	GR	I
IR-6	Incident Reporting	NS	GVR	GVR	GVR	GVR	I
MA-2	Controlled Maintenance	GV	GV	GV	GV	GV	I

ID	Title	Device Security Class					Responsibility (Manufacturer (M); IOO (I))
		1	2	3	4	5	
MA-3	Maintenance Tools	GV	GV	GV	GV	GV	I
MA-3(6)	Software Updates and Patches	G	G	G	G	G	I
MA-4	Nonlocal Maintenance	G	G	G	G	G	M/I
MA-4(1)	Logging and Review	GV	GV	GV	GV	GV	M/I
MA-4(4)	Authentication and Separation of Maintenance Sessions	GVR	GVR	GVR	GVR	GVR	M/I
MA-6	Timely Maintenance	GV	GV	GV	GV	GV	M/I
PE-2	Physical Access Authorizations	GV	GV	GV	GV	GV	I
PE-2(1)	Access by Position or Role	G	G	G	G	G	I
PE-3	Physical Access Control	GVR	GVR	GVR	GVR	GVR	M/I
PE-3(1)	System Access	GV	GV	GV	GV	GV	I
PE-3(4)	Lockable Casings	GV	GV	GV	GV	GV	M/I
PE-3(5)	Tamper Protection	GVR	GVR	GVR	GVR	GVR	M/I
PE-4	Access Control for Transmission	GVR	GVR	GVR	GVR	GVR	M/I
PE-6	Monitoring Physical Access	NS	NS	NS	GV	GV	M/I
PE-9	Power Equipment and Cabling	G	G	G	G	G	M/I
PE-11	Emergency Power	GV	GV	GV	GV	GV	M/I
PE-14	Environmental Controls	GVR	GVR	GVR	GVR	GVR	M/I

ID	Title	Device Security Class					Responsibility (Manufacturer (M); IOO (I))
		1	2	3	4	5	
PE-14(2)	Monitoring with Alarms and Notifications	NS	NS	NS	GV	GV	M/I
PE-21	Electromagnetic Pulse Protection	NS	NS	NS	NS	GV	M/I
PL-2	System Security and Privacy Plans	GVR	GVR	GVR	GVR	GVR	I
PL-7	Concept of Operations	GVR	GVR	GVR	GVR	GVR	M/I
PM-5	System Inventory	GV	GV	GV	GV	GV	M/I
PM-9	Risk Management Strategy	GVS	GVS	GVS	GVS	GVS	M/I
PM-30	Supply Chain Risk Management Strategy	GV	GV	GV	GV	GV	M/I
PM-30(1)	Suppliers of Critical or Mission-Essential Items	G	G	G	G	G	M/I
RA-3	Risk Assessment	GVS	GVS	GVS	GVS	GVS	M/I
RA-3(1)	Supply Chain Risk Assessment	GV	GV	GV	GV	GV	M/I
RA-5	Vulnerability Scanning	NS	GVR	GVR	GVR	GVR	M/I
RA-5(3)	Vulnerability Scanning Breadth and Depth of Coverage	NS	NS	G	G	G	M/I
RA-7	Risk Response	G	G	G	G	G	M/I
SA-4	Acquisition Process	GR	GR	GR	GR	GR	M/I
SA-4(5)	System, Component, and Service Configurations	GV	GV	GV	GV	GV	M/I

ID	Title	Device Security Class					Responsibility (Manufacturer (M); IOO (I))
		1	2	3	4	5	
SA-4(9)	Functions, Ports, Protocols, and Services in Use	G	G	G	G	G	M/I
SA-5	System Documentation	GV	GV	GV	GV	GV	M/I
SA-8	Security and Privacy Engineering Principles	GV	GV	GV	GV	GV	M/I
SA-9	External System Services	GV	GV	GV	GV	GV	I
SA-9(2)	Identification of Functions, Ports, Protocols, and Services	GV	GV	GV	GV	GV	I
SA-10	Developer Configuration Management	GVR	GVR	GVR	GVR	GVR	M/I
SA-10(1)	Software and Firmware Integrity Verification	GR	GR	GR	GR	GR	M/I
SA-10(3)	Hardware Integrity Verification	GS	GS	GS	GS	GS	M
SA-11	Developer Security Testing and Evaluation	NS	GVR	GVR	GVR	GVR	M/I
SA-11(2)	Threat Modeling and Vulnerability Analysis	NS	GVS	GVS	GVS	GVS	M
SA-11(6)	Attack Surface Reviews	NS	NS	G	G	G	M/I
SA-17	Developer Security and Privacy Architecture and Design	NS	G	G	G	G	M/I
SA-17(6)	Structure For Testing	NS	G	G	G	G	M/I

ID	Title	Device Security Class					Responsibility (Manufacturer (M); IOO (I))
		1	2	3	4	5	
SA-22	Unsupported System Components	GVR	GVR	GVR	GVR	GVR	M/I
SC-2	Separation of System and User Functionality	NS	NS	NS	GR	GR	M
SC-2(1)	Separation of System and User Functionality Interfaces for Non-Privileged Users	NS	NS	NS	NS	G	M
SC-3	Security Function Isolation	GR	GR	GR	GR	GR	M
SC-3(1)	Security Function Isolation Hardware Separation	G	G	G	G	G	M
SC-3(2)	Security Function Isolation Access and Flow Control Functions	NS	NS	G	G	G	M
SC-3(3)	Security Function Isolation Minimize Non-Security Functionality	NS	NS	G	G	G	M
SC-5	Denial-of-service Protection	GVR	GVR	GVR	GVR	GVR	M/I
SC-5(1)	Denial-of-service Protection Restrict Ability to Attack Other Systems	GV	GV	GV	GV	GV	M
SC-5(2)	Denial-of-service Protection Capacity, Bandwidth, and Redundancy	NS	NS	NS	G	G	M
SC-5(3)	Denial-of-service Protection	NS	NS	GV	GV	GV	M/I

ID	Title	Device Security Class					Responsibility (Manufacturer (M); IOO (I))
		1	2	3	4	5	
	Detection and Monitoring						
SC-6	Resource Availability	NS	NS	GV	GV	GV	M
SC-7	Boundary Protection	GVR	GVR	GVR	GVR	GVR	M/I
SC-7(3)	Boundary Protection Access Points	NS	NS	NS	GR	GR	I
SC-7(5)	Boundary Protection Deny by Default — Allow by Exception	NS	NS	NS	GVR	GVR	M/I
SC-7(7)	Boundary Protection Split Tunneling for Remote Devices	NS	NS	NS	GV	GV	M/I
SC-7(14)	Boundary Protection Protect Against Unauthorized Physical Connections	GVS	GVS	GVS	GVS	GVS	M/I
SC-7(15)	Boundary Protection Networked Privileged Access	NS	NS	G	G	G	M/I
SC-7(16)	Boundary Protection Prevent Discovery of System Components	NS	NS	NS	G	G	M
SC-7(18)	Boundary Protection Fail Secure	GR	GR	GR	GR	GR	M
SC-7(19)	Boundary Protection Block Communication from Non-	GV	GV	GV	GV	GV	M/I

ID	Title	Device Security Class					Responsibility (Manufacturer (M); IOO (I))
		1	2	3	4	5	
	Organizationally Configured Hosts						
SC-7(21)	Boundary Protection Isolation of System Components	GVR	GVR	GVR	GVR	GVR	I
SC-7(28)	Boundary Protection Connections to Public Networks	GVR	GVR	GVR	GVR	GVR	I
SC-8	Transmission Confidentiality and Integrity	GVRs	GVRs	GVRs	GVRs	GVRs	M
SC-8(1)	Transmission Confidentiality and Integrity Cryptographic Protection	GVS	GVS	GVS	GVS	GVS	M
SC-10	Network Disconnect	GVR	GVR	GVR	GVR	GVR	M
SC-11	Trusted Path	GV	GV	GV	GV	GV	M
SC-13	Cryptographic Protection	GVRs	GVRs	GVRs	GVRs	GVRs	M
SC-17	Public Key Infrastructure Certificates	GVS	GVS	GVS	GVS	GVS	M/I
SC-23	Session Authenticity	GRS	GRS	GRS	GRS	GRS	M
SC-23(1)	Session Authenticity Invalidate Session Identifiers at Logout	G	G	G	G	G	M
SC-24	Fail in Known State	GVR	GVR	GVR	GVR	GVR	M
SC-28	Protection of Information at Rest	GVRs	GVRs	GVRs	GVRs	GVRs	M

ID	Title	Device Security Class					Responsibility (Manufacturer (M); IOO (I))
		1	2	3	4	5	
SC-28(1)	Protection of Information at Rest Cryptographic Protection	GVR	GVR	GVR	GVR	GVR	M
SC-28(3)	Protection of Information at Rest Cryptographic Keys	GVS	GVS	GVS	GVS	GVS	M/I
SC-35	External Malicious Code Identification	G	G	G	G	G	M/I
SC-39	Process Isolation	NS	NS	GR	GR	GR	M
SC-39(1)	Hardware Separation	NS	NS	G	G	G	M
SC-40	Wireless Link Protection	GVS	GVS	GVS	GVS	GVS	M
SC-41	Port and I/O Device Access	GVR	GVR	GVR	GVR	GVR	M/I
SC-43	Usage Restrictions	NS	GV	GV	GV	GV	M/I
SI-2	Flaw Remediation	GVR	GVR	GVR	GVR	GVR	M/I
SI-3	Malicious Code Protection	VR	VR	VR	VR	VR	M/I
SI-3(4)	Malicious Code Protection Updates Only by Privileged Users						M/I
SI-4	Information System Monitoring	GVR	GVR	GVR	GVR	GVR	M/I
SI-4(4)	System Monitoring Inbound and Outbound Communications Traffic	GV	GV	GV	GV	GV	M/I
SI-4(7)	System Monitoring Automated	NS	NS	GV	GV	GV	M/I

ID	Title	Device Security Class					Responsibility (Manufacturer (M); IOO (I))
		1	2	3	4	5	
	Response to Suspicious Events						
SI-4(14)	System Monitoring Wireless Intrusion Detection	G	G	G	G	G	M/I
SI-7	Software, Firmware, and Information Integrity	VR	VR	VR	VR	VR	M/I
SI-7(1)	Software, Firmware, and Information Integrity Integrity Checks	GVR	GVR	GVR	GVR	GVR	M/I
SI-7(2)	Software, Firmware, and Information Integrity Automated Notifications of Integrity Violations	NS	NS	NS	GVR	GVR	M/I
SI-7(10)	Software, Firmware, and Information Integrity Protection of Boot Firmware	GRS	GRS	GRS	GRS	GRS	M/I
SI-10	Information Input Validation	GVR	GVR	GVR	GVR	GVR	M/I
SI-16	Memory Protection	GVR	GVR	GVR	GVR	GVR	M/I
SR-2	Supply Chain Risk Management Plan	GVS	GVS	GVS	GVS	GVS	M/I
SR-3	Supply Chain Controls and Processes	GV	GV	GV	GV	GV	M/I

ID	Title	Device Security Class					Responsibility (Manufacturer (M); IOO (I))
		1	2	3	4	5	
SR-6	Supplier Assessments and Reviews	GV	GV	GV	GV	GV	M/I
SR-6(1)	Supplier Assessments and Reviews Testing and Analysis	GV	GV	GV	GV	GV	M/I
SR-9	Tamper Resistance and Detection	GR	GR	GR	GR	GR	M/I
SR-10	Inspection of Systems or Components	GV	GV	GV	GV	GV	M/I
SR-12	Component Disposal	GV	GV	GV	GV	GV	I

Chapter 4. Detailed Control Specifications

This chapter provides details on the controls specified in chapter 3. For each control, one or more elements may be provided. The elements are discussed in the following paragraphs. The element or sub-element will be included for a control only if there are values or information relevant to that element or sub-element.

Responsible Party (M/I): Indications for which entity implements a control include Manufacturer (M), IOO (I), or both the Manufacturer and the IOO (M/I).

- Various aspects of a control may be implemented by different roles, depending on whether the control content is technical, non-technical, or a combination of both. Non-technical controls (e.g., policies, procedures, desired security functionality, leadership/management decisions) are most often implemented by the IOO. Within the IOO there may be ITS engineers/ integrators (organic or contracted) who manage some of the non-technical security decisions but more likely manage the bulk of the technical security decisions on behalf of the IOO leadership/management. Technical controls are typically implemented by the system and, therefore, would be levied against a developer (organic or contracted) or a manufacturer/vendor. However, the IOO must often make decisions on the technical aspects of the system and convey those to the manufacturer/vendor for design and implementation. Therefore, some controls are tagged herein as M/I regardless of whether they are tagged in NIST SP 800-53⁽¹⁾ as system or organizational. In this chapter, there are references to the above roles, primarily the manufacturer/vendor and the IOO. Distinctions may be made when it is important to understand if the IOO has primary responsibility.

Justification to Select: A risk-based justification is provided to indicate why the control is selected for this control set. That justification is relevant to a typical instantiation of an DMS (not every possible instantiation) consistent with the assumptions for this control set in Assumptions and Characteristics.” Where appropriate the threat sources, vulnerabilities, and/or predisposing conditions in tables 3–6 Appendix A. Threats, Vulnerabilities, and Predisposing Conditions are referenced (i.e., the selected control/enhancement helps mitigate the threat, vulnerability, and/or predisposing condition).

Guidance: The guidance indicates how a control may be applied to the DMS. In some cases, the guidance for the selected controls and control enhancements must be modified from NIST SP 800-53⁽¹⁾ to address the characteristics of the Protocol Implementation Conformance of the control set and the environments in which the system or components operate.

Parameter Value(s): The control text in NIST SP 800-53⁽¹⁾ may include a parameter (e.g., password length and complexity) that needs to be defined before the control can be implemented. If it is appropriate to define a parameter value (PV) in this control set to support consistency across the ITS community, a recommended value is provided. However, State and local transportation agencies may tailor that value based on system-specific risk or other considerations (e.g., technology capabilities, cost to implement). If it is not appropriate to define a parameter value for all DMS within the scope of this control set, no parameter value entry is included. Organizations within the ITS community must define all remaining parameter values for controls selected for systems within their organization.

- The parameter values are defined to flow within the control text, and their placement/position within the control is noted since the entirety of the control text is not included. For example, #2

indicates the value being provided is for the second parameter value within the control text. Where controls contain multiple paragraphs (e.g., a., b., c.) and subparagraphs within those paragraphs (e.g., a.1., a.2, a.3), then the paragraph/subparagraph to which the value applies is provided.

- If a control has a parameter value in paragraph a. and paragraph c. for which values are being provided, but no parameter value to define for paragraph b., then the notation will identify only paragraph a. and c. and will not contain a reference to paragraph b.
- Where multiple values may be defined within a paragraph or subparagraph, their position will be noted using #1 or #2 as appropriate. If the parameter value contains no annotation regarding its placement, then this indicates there is only one value to define for the control and annotation of its placement within the control is not needed. It should be noted that sometimes a parameter value begins with the word “a” which should not be confused with a paragraph annotation of “a.”
- Parameter values are contextual, and many are typically a suggested minimum, such as “at least annually.” The parameter value should be read in the context of the full control text in NIST SP 800-53⁽¹⁾ to fully understand the meaning.

Risk References and Resources: If there is an authoritative source (e.g., ATT&CK for ICS,⁽³⁴⁾ NIST SP 800-82,⁽³⁾ or ARC-IT⁽¹⁸⁾) that prescribes or recommends a security capability provided by the control, that authoritative source is included in this element.

- For controls selected below for which there is an ATT&CK for ICS mapping, the relevant mitigations and techniques will be listed. Where there is an ATT&CK mapping, only those techniques deemed relevant to the typical DMS implementation are listed, as not every technique is feasible or possible against a typical DMS. However, system owners may consider the relevance of other techniques based on their specific system architecture, design, or use. This control set and the related mitigations and techniques are only a starting point from which system owners must tailor controls in or out based on a risk assessment.
- NIST SP 800-82⁽³⁾ includes an “Operational Technically (OT) Discussion” for some controls in its overlay for OT. Those discussions are included if relevant to the DMS, but wording may be adapted (e.g., replacing OT with ITS) to the unique features or functions of the DMS.
- The ARC-IT Mechanisms are requirements-like statements that could be conveyed to a manufacturer/vendor for DMS design and implementation.

Standards: This element lists standards relevant to the DMS that prescribe capabilities or cybersecurity requirements.

AC Family – Access Control

AC-1, Policy and Procedures

Responsible Party (M/I): I

Justification to Select: Vulnerability “Inadequate security policy for ITS” in table 6, Policy and Procedure Vulnerabilities and Predisposing Conditions. The establishment, maintenance, and dissemination of access control policies and procedures is part of the governance required to manage the cybersecurity risks of an IOO. It is a prerequisite to the implementation and lifecycle management of cybersecurity protections and safeguards for ITS.

Guidance: This is an organizational control, as the IOO (not the manufacturer), would create the policies and procedures. If the IOO does not have access control policies and procedures, the

integrator, engineers, or developers may have no direction or guidance to design, develop, and manage access control capabilities in the DMS. This control is not implemented on or by the DMS itself, but the IOO develops, publishes, and conveys to the manufacturer/vendor key access control policies and procedures to guide implementation of other access controls from this family on the DMS.

Parameter Value(s):

paragraph a. "CISO, Security Admins, domain admins, and any other pertinent personnel or roles"

paragraph a.1. "System-level

paragraph c.1. #1 "at least annually"

paragraph c.1. #2 "device or vendor onboarding, security incidents, intrusion detections, changes to the DMS system or controller database configuration, or changes to the DMS control set."

paragraph c.2. #1 at least annually"

paragraph c.2. #2 "device or vendor onboarding, security incidents, intrusion detections, changes to the DMS system or controller database configuration, or changes to the DMS control set."

Risk References and Resources:

NIST SP 800-82⁽³⁾ The policy specifically addresses the unique properties and requirements of ITS and the relationship to non-ITS systems. ITS access by vendors and maintenance staff can occur over a large facility footprint or geographic area and into unobserved spaces such as mechanical/electrical rooms and field substations.

AC-2, Account Management

Responsible Party (M/I): I

Justification to Select: Vulnerability "Inadequate access controls applied" in table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: The IOO establishes and manages accounts that provide access to DMS control software, message libraries, controller configuration databases, and remote maintenance interfaces. The IOO assigns accounts according to defined operational roles, including message creation, message approval, message deployment, monitoring, and administrative functions. The IOO provisions, modifies, disables, and removes accounts in accordance with organizational policy and operational requirements and ensures that access reflects the user's job title or operational role.

The IOO manages vendor and contractor accounts used for DMS maintenance as uniquely identifiable accounts and restricts their use to authorized maintenance activities. The manufacturer provides account management capabilities within the DMS control software and, where supported, within the field controller. The system supports role-based access differentiation and administrative control of account status consistent with the IOO's policy.

Parameter Value(s):

paragraph c. "completion of security awareness training, valid need-to-know justification, written supervisor approval, and/or current background check."

paragraph d.3. "access level (e.g., read-only, full access, access to update the controller database, etc.)"

paragraph f. "Account Management Policy"

paragraph h. "Security Admins, domain admins, HR,"

paragraph h.1. "24 hours"

paragraph h.2. "24 hours"

paragraph h.3. "24 hours"

paragraph i.3. "Job title or operational role"

paragraph j. "quarterly"

Risk References and Resources:

NIST SP 800-82:⁽³⁾ In ITS systems, physical security, personnel security, intrusion detection, or auditing measures may support this control objective.

ATT&CK for ICS Mitigations / Techniques:

- M0918 / T0822, T0838, T0886, T0881, T0859
- M0926 / T0809, T0811, T0866, T0842, T0859

AC-2(3), Account Management | Disable Accounts

Responsible Party (M/I): M/I

Justification to Select: Vulnerability "Inadequate access controls applied" in table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: The IOO disables accounts when they are no longer required, when users separate from the organization, or when temporary or emergency access is no longer needed. The IOO disables vendor and contractor accounts used for DMS maintenance immediately upon completion of authorized maintenance activities. The manufacturer provides the capability within the DMS control software, and where technically feasible within the field controller, to disable accounts or otherwise prevent further authentication. Where local controller functionality is limited, the IOO enforces account disabling through centralized DMS control software or network access controls.

Parameter Value(s):

#1 "immediately upon completion of authorized activity, not to exceed 24 hours."

paragraph d. "90 days"

Risk References and Resources:

NIST SP 800-82:⁽³⁾ When the ITS (e.g., field devices) cannot support temporary or emergency accounts, this enhancement does not apply. Example compensating controls include employing non-automated mechanisms or procedures.

Standards: NIST SP 800-82

AC-2(4), Account Management | Automated Audit Actions

Responsible Party (M/I): I

Justification to Select: Non-adversarial threat event "Incorrect privilege settings" in table 4.

Guidance: The IOO configures DMS control software or supporting systems to generate audit records when accounts are created, modified, disabled, or granted elevated privileges. The IOO ensures that changes affecting access to message control functions, controller configuration databases, or administrative capabilities are auditable. The manufacturer provides the capability within the DMS control software to support automated audit logging of account management actions.

AC-2(5), Account Management | Inactivity Logout

Responsible Party (M/I): M/I

Justification to Select: Vulnerability "Inadequate access controls applied" in table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: The IOO requires users to log out of DMS management interfaces when their duties are complete or when leaving the workstation. The requirement applies to TMC workstations accessing DMS control software, web-based DMS management interfaces, and remote maintenance sessions. The manufacturer provides a logout capability within all DMS user interfaces to support enforcement of the IOO's policy. Automatic session termination due to inactivity is addressed under AC-11.

Parameter Value(s):

"their duties are complete, they physically leave the system, or they expect to be inactive for more than ten minutes"

Risk References and Resources:

NIST SP 800-82:⁽³⁾ This control enhancement defines situations or timeframes in which users log out of accounts in policy; automatic enforcement is not addressed by this control enhancement (see AC-11). Organizations determine if this control enhancement is appropriate for the mission and/or functions of the ITS system and define the timeframe or scenarios. If no timeframe or scenario(s) apply, the organization-defined parameter reflects as such.

Standards: ISO 27001

AC-3, Access Enforcement

Responsible Party (M/I): M/I

Justification to Select: Threat event "Obtain unauthorized access" in table 3, Achieve Results (i.e., cause adverse impacts, obtain information).

Guidance: The IOO enforces access restrictions on DMS control software, controller configuration data, and maintenance interfaces to ensure that only authorized users can perform actions consistent with their assigned roles. The IOO defines which operational roles are permitted to monitor system status, create and deploy messages, modify controller configuration data, and perform administrative functions.

The manufacturer provides role-based access control capabilities within the DMS control software that restrict actions based on authenticated user identity and assigned role. The system enforces access control prior to permitting configuration changes or transmission of commands to the sign controller.

Risk References and Resources:

NIST SP 800-82:⁽³⁾ The organization ensures that access enforcement mechanisms do not adversely impact the operational performance of the ITS. Example compensating controls include encapsulation. The policy for logical access control to non-addressable and non-routable system resources and the associated information is made explicit. Access control mechanisms include hardware, firmware, and software that control the device or have device access, such as device drivers and communications controllers. Physical access control may serve as a compensating control for logical access control. However, it may not provide sufficient granularity when users require access to different functions.

ATT&CK for ICS Mitigations / Techniques:

- M0800 / T0800, T0858, T0868, T0816, T0871, T0838, T0836, T0843, T0845, T0886
- M0801 / T0800, T0858, T0812, T0868, T0816, T0871, T0891, T0838, T0839, T0843, T0845, T0886, T0857, T0859
- M0807 / T0800, T0878, T0802, T0803, T0804, T0805, T0806, T0858, T0879, T0868, T0816, T0838, T0839, T0861, T0843, T0845, T0886, T0848, T0856, T0869, T0857, T0855
- M0930 / T0800, T0830, T0878, T0802, T0805, T0806, T0858, T0885, T0868, T0816, T0819, T0866, T0822, T0838, T0839, T0842, T0861, T0843, T0845, T0886, T0848, T0881, T0856, T0869, T0857, T0864, T0855
- M0935 / T0822
- M0937 / T0800, T0806, T0884, T0868, T0816, T0839, T0861, T0843, T0845, T0886, T0848, T0856, T0857, T0855, T0859

AC-3(2), Access Enforcement | Dual Authorization

Responsible Party (M/I): I

Justification to Select: Threat event "Obtain unauthorized access" in table 3, Achieve Results (i.e., cause adverse impacts, obtain information).

Guidance: The IOO implements dual authorization for defined high-risk actions within the DMS control environment where operationally feasible. The IOO identifies which actions require approval by two authorized individuals prior to execution. Such actions may include controller configuration changes, firmware updates, or establishment of remote maintenance access.

When supported, the IOO configures the DMS control software to enforce dual authorization through workflow controls.

Parameter Value(s):

"controller configuration changes, firmware updates, and remote maintenance access."

AC-3(4), Access Enforcement | Discretionary Access Control

Responsible Party (M/I): M/I

Justification to Select: Threat event "Obtain unauthorized access" in table 3, Achieve Results (i.e., cause adverse impacts, obtain information).

Guidance: The IOO defines policies governing how access permissions are assigned within the DMS control software. The IOO restricts the authority to grant, modify, or revoke user access to designated administrative roles.

The manufacturer provides configurable access control functionality within the DMS control software that allows authorized administrators to assign users to predefined roles and manage associated permissions. The system prevents non-administrative users from granting access privileges or modifying role assignments.

AC-4, Information Flow Enforcement

Responsible Party (M/I): M/I

Justification to Select: Threat event "Obtain sensitive information through network sniffing of external networks" in table 3, Conduct an Attack (i.e., direct/coordinate attack tools or activities).

Guidance: The IOO defines information flow control policies governing communications between the DMS control software, sign controllers, and connected networks. The IOO restricts communications to authorized source and destination addresses, ports, and protocols necessary for DMS operations and maintenance.

The IOO implements network segmentation to separate DMS systems from enterprise networks and other external systems. The IOO configures firewalls, managed switches, or other boundary devices to permit only authorized communications to and from the DMS control software and associated field devices.

The manufacturer supports secure implementation of communications interfaces within the DMS control software and sign controller and ensures that only required services and protocols are enabled.

Parameter Value(s):

"network segmentation and firewall policies that restrict communications between the TMC and field devices to authorized IP addresses, ports, protocols, and encrypted tunnels."

Risk References and Resources:

NIST SP 800-82:⁽³⁾ Information flow policy may be achieved using a combination of logical and physical flow restriction techniques. Inspection of message content may enforce information flow policy. For example, ITS protocols may be restricted using inbound and outbound traffic rules on a network control device between ITS and TMC networks. For non-routable communication such as serial connections, devices may be configured to limit commands to and from specific tags within the ITS device. Information flow policy may be supported by labeling or coloring physical connectors to aid in connecting networks. Devices that do not have a business need to communicate should not be connected (i.e., air gapped).

ATT&CK for ICS Mitigations / Techniques:

- M0807 / T0803, T0804, T0884, T0869, T0855
- M0930 / T0830, T0805, T885, T0868, T0842

AC-4(4), Information Flow Enforcement | Flow Control of Encrypted Information

Responsible Party (M/I): M/I

Justification to Select: Threat event "Obtain sensitive information through network sniffing of external networks" in table 3, Conduct an Attack (i.e., direct/coordinate attack tools or activities).

Guidance: The IOO configures boundary devices to restrict encrypted sessions to authorized endpoints and services. The manufacturer supports the use of encrypted communications protocols within the DMS control software and sign controller consistent with the IOO's security policies.

Parameter Value(s):

#1 "boundary protection devices configured to enforce security policy on encrypted sessions, including filtering by authorized endpoints and services."

AC-5, Separation of Duties

Responsible Party (M/I): M/I

Justification to Select: Vulnerability "Inadequate access controls applied" in table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: Both the manufacturer and IOO should ensure that separation of sensitive controls and duties related to operating the DMS control software or actions within the sign controller is enforced to prevent unauthorized modifications and maintain the integrity of traffic information displayed to the public. This includes maintaining distinct roles for functions such as message creation and scheduling, system configuration, access control administration, and audit monitoring, ensuring no individual holds overlapping responsibilities that could enable misuse or unauthorized changes to the DMS.

Parameter Value(s):

"system operators who approve messages, system admins who configure the hardware, and security personnel who monitor access logs"

Risk References and Resources:

NIST SP 800-82:⁽³⁾ Example compensating controls include providing increased personnel security and auditing.

AC-6, Least Privilege

Responsible Party (M/I): I

Justification to Select: The principle of least privilege (POLP) is a fundamental security concept of giving a user account or process only those privileges which are essential to perform its intended function. Applying POLP reduces the risk of attackers gaining access to critical systems or sensitive data by compromising a low-level user account, device, or application.

Guidance: The IOO implements the principle of least privilege within the DMS control environment by assigning users only the access necessary to perform their defined operational duties. The IOO defines distinct roles for monitoring, message creation, message deployment, controller configuration, and administrative functions and assigns privileges accordingly.

The IOO restricts administrative privileges to designated personnel and ensures that users performing routine operational tasks do not have configuration or system management capabilities unless explicitly required. The IOO also restricts vendor and maintenance access to only those functions necessary for authorized maintenance activities.

Risk References and Resources:

NIST SP 800-82: Example compensating controls include providing increased personnel security and auditing. The organization carefully considers the appropriateness of a single individual having multiple critical privileges. System privilege models may be tailored to enforce integrity and availability (e.g., lower privileges include read access and higher privileges include write access).

ATT&CK for ICS Mitigations / Techniques:

- M092/T0809, T0811, T0872, T0849, T0873, T0881, T0882

AC-6(1), Least Privilege | Authorize Access to Security Functions

Responsible Party (M/I): M/I

Justification to Select: Non-adversarial threat event "Incorrect privilege settings" in table 4.

Guidance: The IOO defines the security functions within the DMS control environment that require explicit authorization and identifies the roles permitted to perform those functions. Security functions may include management of user accounts and roles, modification of controller configuration data, firmware updates, access to audit logs, modification of network settings, and other actions that affect system integrity or availability.

The IOO defines the security-relevant information that requires restricted access and communicates these requirements to the manufacturer.

The manufacturer provides mechanisms within the DMS control software and controller interfaces that restrict access to defined security functions based on authenticated role and prevent unauthorized users from performing administrative or security-sensitive actions.

Parameter Value(s):

"Local Administrators, Field Technicians, Remote Administrators, and Vendors."

paragraph a. "physically access the controller interface for device setup and diagnostics, perform firmware verification, configure network addressing, and load organization-approved firmware images."

paragraph b. "firmware version information, configuration data, audit logs, device certificates where implemented, network configuration settings, user access permissions, and security event logs."

Risk References and Resources:

NIST SP 800-82:⁽³⁾ In situations where the ITS components (e.g., programmable logic controllers [PLC]) cannot support logging of privileged functions, other system components within the authorization boundary may be used (e.g., engineering workstations or physical access monitoring).

AC-6(3), Least Privilege | Network Access to Privileged Commands

Responsible Party (M/I): I

Justification to Select: Non-adversarial threat event "Incorrect privilege settings" in table 4.

Guidance: The IOO identifies privileged commands within the DMS control environment that may be executed over a network connection and documents the operational justification for allowing remote execution of those commands. The IOO restricts network access to such privileged commands to authorized roles and ensures that remote execution is necessary for operational continuity or safety.

Parameter Value(s):

#1 "commands or functions that can alter the DMS's operational state or security configuration"

#2 "operational needs where local access is infeasible or would adversely affect system availability or roadway safety."

Risk References and Resources:

NIST SP 800-82:⁽³⁾ In situations where the ITS components (e.g., DMS) cannot support logging of privileged functions, other system components within the authorization boundary may be used (e.g., engineering workstations or physical access monitoring).

AC-6(8), Least Privilege | Privilege Levels for Code Execution

Responsible Party (M/I): MI

Justification to Select: Vulnerability "Inadequate authentication, privileges, and access control in software" in table 6, Software Development Vulnerabilities and Predisposing Conditions.

Guidance: The manufacturer designs DMS operating systems and application components so that software executes with only the privileges necessary for its intended function. The manufacturer ensures that application processes do not execute with administrative or root privileges unless required for specific, authorized maintenance or update functions.

The IOO requires, through procurement or system acceptance criteria, that DMS software components enforce separation between application-level functions and underlying system-level privileges.

The manufacturer implements controls that prevent unauthorized privilege escalation and ensures that firmware updates and maintenance utilities operate through authorized and auditable mechanisms.

Parameter Value(s):

"DMS operating system services and application components execute only with the privileges required for their assigned function. Execution with root or administrative privileges is restricted to organization-approved and authenticated maintenance or firmware update processes."

AC-6(10), Least Privilege | Prohibit Non-Privileged Users from Executing Privileged Functions

Responsible Party (M/I): M/I

Justification to Select: Vulnerability "Inadequate authentication, privileges, and access control in software" in table 6, Software Development Vulnerabilities and Predisposing Conditions.

U.S. Department of Transportation
Office of the Assistant Secretary for Research and Technology
Intelligent Transportation Systems Joint Program Office

Guidance: The IOO defines the set of privileged functions within the DMS control environment, including configuration changes, firmware updates, user management, and security setting modifications. The IOO restricts execution of these functions to authorized roles.

The manufacturer implements controls within the DMS control software and controller interfaces that prevent non-privileged users from executing defined privileged functions. The system enforces role validation prior to execution of any privileged action.

Risk References and Resources:

NIST SP 800-82:⁽³⁾ Example compensating controls include enhanced auditing.

ARC-IT Mechanisms: See AC-06.

AC-7, Unsuccessful Logon Attempts

Responsible Party (M/I): M/I

Justification to Select: Threat event “Conduct brute force login attempts/password guessing attacks” in table 3, Conduct an Attack (i.e., direct/coordinate attack tools or activities).

Guidance: The IOO defines the number of consecutive invalid logon attempts permitted for accounts accessing the DMS control software and any locally accessible controller interfaces. The IOO also defines the time period during which invalid attempts are counted and the automated actions taken when the defined threshold is exceeded.

The manufacturer implements account lockout or equivalent protective mechanisms within the DMS control software and, where supported, within the controller interface. The system enforces lockout or other protective action even when operating without connectivity to a centralized management system.

Parameter Value(s):

paragraph a. #1 “5”

paragraph a. #2 “15 minutes”

paragraph b. “lock the account or node until released by an administrator; notify system administrator”

Risk References and Resources:

NIST SP 800-82:⁽³⁾ Many ITS remain in continuous operation and operators remain logged onto the system continuously. A “log-over” capability may be employed. Example compensating controls include logging or recording all unsuccessful login attempts and alerting ITS security personnel through alarms or other means when the number of organization-defined consecutive invalid access attempts is exceeded. Unsuccessful logon attempt limits are enforced for accounts (e.g., administrator) or systems (e.g., engineering workstations) not required for continuous operation.

ATT&CK for ICS Mitigations / Techniques:

- M0927 / T0892, T0812, T0822, T0886, T0859

AC-8, System Use Notification

Responsible Party (M/I): M/I

Justification to Select: Threat Event "Perform reconnaissance and surveillance of targeted organizations" in table 3, Perform Reconnaissance and Gather Information.

Guidance: The IOO requires a system use notification banner to be displayed prior to granting access to the DMS control software. The notification informs users that the system is for authorized use only, that activity may be monitored and recorded, and that unauthorized use may result in disciplinary or legal action.

The manufacturer implements the capability within the DMS control software to display the system use notification for all interactive login sessions.

Parameter Value(s):

paragraph c.1. "for all interactive login sessions"

Risk References and Resources:

NIST SP 800-82:⁽³⁾ Many ITS remain in continuous operation and operators remain logged onto the system continuously. A "log-over" capability may be employed. Example compensating controls include logging or recording all unsuccessful login attempts and alerting ITS security personnel through alarms or other means when the number of organization-defined consecutive invalid access attempts is exceeded. Unsuccessful logon attempt limits are enforced for accounts (e.g., administrator) or systems (e.g., engineering workstations) not required for continuous operation.

AC-9, Previous Logon Notification

Responsible Party (M/I): I

Justification to Select: Threat event "Conduct brute force login attempts/password guessing attacks" in table 3, Conduct an Attack (i.e., direct/coordinate attack tools or activities).

Guidance: The manufacturer provides the capability within the DMS control software, and where supported within local controller interfaces, to display information regarding the date and time of the last successful logon and any unsuccessful logon attempts since the previous successful logon.

The IOO trains administrators and technicians to report suspicious or unexpected previous logon notifications in accordance with incident response procedures.

Risk References and Resources:

ATT&CK for ICS Mitigations / Techniques:

- M0919 / T0863

AC-10, Concurrent Session Control

Responsible Party (M/I): M/I

Justification to Select: Vulnerability "Inadequate authentication, privileges, and access control in software" in table 6, Software Development Vulnerabilities and Predisposing Conditions.

Guidance The IOO defines limits on the number of concurrent sessions permitted for each account type within the DMS control software. The IOO ensures that concurrent session limits reduce the risk of credential sharing, unauthorized simultaneous access, or administrative misuse.

The manufacturer implements configurable concurrent session controls within the DMS control software and enforces these limits even when operating without connectivity to a centralized management system.

Parameter Value(s):

#1 “Administrator, Maintenance, Vendor, and Operator accounts.”

#2 “one concurrent session for Administrator, Maintenance, and Vendor accounts; two concurrent sessions for Operator accounts.”

Risk References and Resources:

NIST SP 800-82:⁽³⁾ The number, account type, and privileges of concurrent sessions consider the roles and responsibilities of the affected individuals. Example compensating controls include providing increased auditing measures.

AC-11, Device Lock

Responsible Party (M/I): M/I

Justification to Select: Threat event “Theft of Operational Information” in table 5, Physical Object Threat Events.

Guidance: The IOO defines device lock requirements for workstations and interfaces used to access the DMS control software. The IOO establishes inactivity time thresholds and requirements for user-initiated locking when leaving a workstation unattended.

The manufacturer provides the capability within the DMS control software to automatically lock interactive sessions after a defined period of inactivity and to allow users to manually lock their session. The system permits other authorized users to authenticate and establish independent sessions without interfering with a previously locked session.

Parameter Value(s):

paragraph a. “initiating a device lock after no more than 15 minutes of inactivity, requiring the user to initiate a device lock before leaving the system unattended”

Risk References and Resources:

NIST SP 800-82:⁽³⁾ This control assumes a staffed environment where users interact with system displays. This control may be tailored appropriately where systems do not have displays configured, systems are placed in an access-controlled facility or locked enclosure, or immediate operator response is required in emergency situations. Example compensating controls include locating the display in an area with physical access controls that limit access to individuals with permission and need-to-know for the displayed information.

ATT&CK for ICS Mitigations / Techniques:

- M0922 / T0809, T0811, T0893, T0849, T0873, T0881, T0822

AC-12, Session Termination

Responsible Party (M/I): M/I

Justification to Select: Threat event "Theft of Operational Information" in table 5, Physical Object Threat Events.

Guidance: The IOO defines conditions requiring termination of user sessions within the DMS control environment. The IOO specifies inactivity time thresholds, logout requirements, and conditions requiring forced session termination, including administrative action or detection of suspicious activity.

The manufacturer provides configurable session termination capabilities within the DMS control software and ensures that terminated sessions invalidate active session identifiers to prevent reuse.

Parameter Value(s):

"15 minutes of inactivity, explicit user logout, administrative termination, detection of a security event, or expiration of authorized remote access window."

Risk References and Resources:

NIST SP 800-82:⁽³⁾ Example compensating controls include providing increased auditing measures or limiting remote access privileges to key personnel.

ATT&CK for ICS Mitigations / Techniques:

- M0922 / T0809, T0811, T0893, T0849, T0873, T0881, T0822

AC-12(1), Session Termination | User-Initiated Logouts

Responsible Party (M/I): M

Justification to Select: Threat event "Conduct externally based session hijacking" in table 3, Conduct an Attack (i.e., direct/coordinate attack tools or activities).

Guidance: The manufacturer implements a logout capability for all authenticated DMS control software interfaces. The logout function immediately terminates the active session and invalidates any associated session identifiers to prevent reuse or hijacking. Logout functionality is provided for all interfaces supporting interactive user authentication.

Parameter Value(s):

"provide a user-initiated logout capability for all authenticated DMS control software interfaces that immediately terminates the session and invalidates associated session identifiers."

AC-14, Permitted Actions without Identification or Authentication

Responsible Party (M/I): M/I

Justification to Select: Threat event "Obtain unauthorized access" in table 3, Achieve Results (i.e., cause adverse impacts, obtain information).

Guidance: The manufacturer ensures that all configuration, administrative, and message control functions require authentication. The system restricts unauthenticated access to non-sensitive display or status information only, where explicitly authorized by the IOO.

Parameter Value(s):

“publicly viewable status or informational displays that do not permit configuration changes or message modification.”

AC-16, Security and Privacy Attributes

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Inadequate organizational ownership of risk assessments” in table 6, Conduct an Attack (i.e., direct/coordinate attack tools or activities).

Guidance: The IOO defines categories of information processed or stored within the DMS control environment, including operational data, configuration data, audit logs, and user account information. The IOO defines handling requirements for each category, including access restrictions and retention requirements, and documents these in the system security plan. Where cryptographic protections are implemented, the manufacturer ensures that encryption mechanisms meet applicable federal or organizational requirements.

Parameter Value(s):

paragraph a. #1 “information category; retention period; authorized access role; cryptographic protection requirement.”

paragraph a. #2 “{Operational Data, Configuration Data, Audit Logs, User Account Information}; {Operator, Administrator, Maintenance, Vendor}; {IOO-defined retention periods}; {Required, Not Required}.”

paragraph c. #1 “DMS control software and associated storage components.”

paragraph c. #2 “information category and authorized access role.”

paragraph d. “information categories limited to Operational Data, Configuration Data, Audit Logs, and User Account Information; access roles limited to Operator, Administrator, Maintenance, and Vendor; retention periods limited to IOO-defined ITS data retention policies; cryptographic protection requirement limited to Required or Not Required as defined by IOO policy.”

paragraph f. #1 “information category; authorized access role; retention period; cryptographic protection requirement.”

paragraph f. #2 “annually or upon system configuration change or introduction of new data types.”

Standards: ISO 27002:2022 Control 5.12 - Classification of Information, ISO 27002:2022 Control 5.13 - Labelling of Information, FIPS 199, FIPS 140-3

AC-17, Remote Access

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Poor remote access controls” in table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: The IOO defines policies governing remote access to the DMS control software and associated maintenance interfaces, including authorized users, approved access methods, authentication requirements, time-of-day restrictions, and monitoring expectations.

The manufacturer provides the capability to enforce remote access policies using secure, encrypted communications channels. Remote access sessions use strong, organization-approved cryptographic mechanisms and mutual authentication where technically feasible.

Remote access is restricted to authorized operational or maintenance purposes and is permitted only through approved access paths. The IOO ensures that remote access mechanisms use cryptographic modules that meet applicable federal or organizational requirements.

Where the DMS participates in connected vehicle or cooperative ITS environments, remote communications interfaces align with applicable ITS security standards, including ISO 21177, as required by the IOO.

Risk References and Resources:

NIST SP 800-82:⁽³⁾ In situations where the ITS cannot implement any or all of the components of this control, the organization employs other mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

ATT&CK for ICS Mitigations / Techniques:

- M0935 / T0822

AC-17(1), Remote Access | *Monitoring and Control*

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Poor remote access controls” in table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: The IOO establishes procedures to monitor and control remote access sessions to the DMS control environment. The IOO defines logging requirements for remote session establishment, authentication events, privilege escalation, and session termination.

The manufacturer enables the DMS control software to log remote access session initiation, termination, authentication success or failure, and administrative actions performed during remote sessions. Audit records are retained and reviewed in accordance with organizational monitoring policies.

Risk References and Resources:

NIST SP 800-82:⁽³⁾ Example compensating controls include employing non-automated mechanisms or procedures as compensating controls. Compensating controls could include limiting remote access to a specified period or placing a call from the ITS site to the authenticated remote entity.

AC-17(2), Remote Access | *Protection of Confidentiality and Integrity Using Encryption*

Responsible Party (M/I): M

Justification to Select: Vulnerability “Poor remote access controls” in table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: The manufacturer supports encrypted remote access sessions that protect the confidentiality and integrity of communications between remote users and the DMS control software.

Remote sessions use strong, industry-recognized cryptographic protocols and support mutual authentication where required by organizational policy.

Where applicable, cryptographic implementations align with federal or organizational requirements. If the DMS participates in cooperative ITS communications, security services may align with ISO 21177 profiles as specified by the IOO.

Risk References and Resources:

Encryption-based technologies should be used to support the confidentiality and integrity of remote access sessions. While ITS devices often lack the ability to support modern encryption, additional devices (e.g., virtual private networks) can be added to support these features. This control should not be confused with SC-8 – Transmission Confidentiality and Integrity, which discusses confidentiality and integrity requirements for general communications, including between ITS devices.

Standard: NTCIP 1203 v03, Section 4⁽⁵⁾; Request For Comment (RFC) 8446 ⁽³⁶⁾

AC-18, Wireless Access

Responsible Party (M/I): I

Justification to Select: Vulnerability “Unauthorized wireless access to sensors or final elements” in table 6, Sensor, Final Element, and Asset Management Vulnerabilities and Predisposing Conditions. Threat event “Install general-purpose sniffers on organization controlled information systems or networks” in table 3, Deliver/Insert/Install Malicious Capabilities.

Guidance: The IOO defines policy governing the use or prohibition of wireless capabilities within the DMS control environment and associated field controllers. The IOO identifies approved wireless technologies, authorized use cases, and configuration requirements.

The manufacturer provides the capability to enable or disable wireless functionality within the DMS control software and controller interfaces. Wireless interfaces that are not required for operations or maintenance are disabled by default or capable of being disabled by the IOO.

Risk References and Resources:

NIST SP 800-82:⁽³⁾ In situations where ITS cannot implement any or all the components of this control, the organization employs other mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

ARC-IT Mechanisms:

- See AC-01, AC-03, AC-06.
- Only high-privileged users explicitly identified will have permission to modify wireless configurations. See AC-03.
- Appropriately tune wireless antennas in an organization or make use of directional antennas to only propagate wireless signals within the physical confines of the organization.

AC-18(1), Wireless Access | Authentication and Encryption

Responsible Party (M/I): M

Justification to Select: Vulnerability “Inadequate authentication between wireless clients and access points” in table 6, Communication and Network Configuration Vulnerabilities and Predisposing Conditions.

Guidance: The manufacturer ensures that wireless communications supported by the DMS control software or controller interfaces provide authentication of users or devices, as applicable, and protection of data confidentiality and integrity using industry-recognized cryptographic mechanisms.

Wireless client connections require authentication prior to granting access to configuration or control functions.

Parameter Value(s):

"users; devices"

Risk References and Resources:

NIST SP 800-82:⁽³⁾ Implementation of authentication and encryption is driven by the ITS environment. There are some scenarios where devices and users cannot all be authenticated and encrypted due to operational or technology constraints. In such scenarios, compensating controls include providing increased auditing for wireless access, limiting wireless access privileges to key personnel, or using AC-18 (05) to reduce the boundary of wireless access.

ARC-IT Mechanisms: See AC-18.

Standard: NTCIP 9014 v01.20, Annex B.⁽³⁹⁾

AC-18(3), Wireless Access | Disable Wireless Networking

Responsible Party (M/I): M/I

Justification to Select: Wireless access increases the DMS attack surface. If the IOO does not intend to use wireless networking, this control should be applied to prevent its use.

Guidance: The IOO disables wireless networking capabilities within the DMS control environment and controller interfaces when wireless communication is not operationally required.

The manufacturer provides the capability to disable embedded wireless radios or wireless services through configuration settings or physical controls.

AC-18(5), Wireless Access | Antennas and Transmission Power Levels

Responsible Party (M/I): I

Justification to Select: Threat event “Install general-purpose sniffers on organization controlled information systems or networks” in table 3, Deliver/Insert/Install Malicious Capabilities.

Guidance: When wireless functionality is authorized and transmission power levels or antenna characteristics are configurable, the IOO configures transmission power and antenna placement to limit signal propagation to the minimum necessary for operational or maintenance purposes. The IOO ensures that wireless coverage does not unnecessarily extend beyond the intended operational boundary. If wireless parameters are not configurable, the IOO selects equipment and deployment locations that appropriately limit unintended signal exposure. For field-deployed DMS that rely on cellular communications, the IOO ensures that only organization-approved carrier services and device configurations are used.

Risk References and Resources:

NIST SP 800-82:⁽³⁾ Availability and interference for wireless signals may be a concern within ITS environments. Antennas and power levels should be designed to overcome and achieve availability goals. Where confidentiality is concerned, antennas and power levels can also be designed to minimize signal exposure outside of the facility.

AC-20, Use of External Systems

Responsible Party (M/I): M/I

Justification to Select: Threat event “Coordinate cyberattacks using external (outsider), internal (insider), and supply chain (supplier) attack vectors” in table 3, Coordinate a Campaign.

Guidance: The IOO defines the conditions under which external systems are permitted to access or interface with the DMS control environment. The IOO identifies authorized external systems, acceptable connection methods, required security controls, and monitoring expectations. The IOO documents trust relationships for external systems, including vendor support systems and contractor-managed devices, and ensures that risks associated with such connections are formally accepted and managed. The manufacturer provides configuration capabilities within the DMS control software and controller interfaces that allow the IOO to restrict, permit, or condition connections from external systems in accordance with organizational policy.

Parameter Value(s):

paragraph a. “multi-factor authentication where feasible, encryption of data in transit, logging of access events, and periodic vulnerability assessment of remote access pathways.”

paragraph b. “personally owned devices, unmanaged laptops, and external storage devices not explicitly authorized for DMS maintenance.”

Risk References and Resources:

NIST SP 800-82:⁽³⁾ Organizations refine the definition of “external” to reflect lines of authority and responsibility; granularity of organization entity; and their relationships. An organization may consider a system to be external if that system performs different functions, implements different policies, falls under different management authorities, or does not provide sufficient visibility into the implementation of controls to allow the establishment of a satisfactory trust relationship. For example, an ITS and a business data processing system may be considered external to each other depending on the organization’s system boundaries. Access to an ITS for support by a business partner, such as a vendor or support contractor, is another common example. The definition and trustworthiness of external systems is re-examined with respect to ITS functions, purposes, technology, and limitations to establish a clearly documented technical or business case for use and an acceptance of the risk inherent in the use of an external system.

ATT&CK for ICS Mitigations / Techniques:

- M0801 / T0868, T0886

Standards: FIPS 140-3⁽⁸⁾, NIST SP 800-46

AC-20(1), Use of External Systems | Limits on Authorized Use

Responsible Party (M/I): I

Justification to Select: If external systems are authorized for use, the IOO needs to establish and document clear limits on their use as well as accepting the risk inherent in the use of external systems.

Guidance: The IOO establishes and documents limits on the authorized use of approved external systems that access the DMS control environment. The IOO specifies permitted functions, timeframes, user roles, and access methods for each authorized external system.

AC-20(2), Use of External Systems | Portable Storage Devices – Restricted Use

Responsible Party (M/I): I

Justification to Select: If external systems are authorized for use, the IOO needs to determine what restrictions should be applied to use of portable storage devices (e.g., USB drives) with DMS storage devices are a common way to compromise a system.

Guidance: The IOO establishes policy governing the use of portable storage devices with DMS control software and field controllers. The IOO limits or prohibits the use of portable media except during authorized maintenance activities performed by designated personnel.

When portable media use is authorized, the IOO requires that media be scanned for malware on a trusted system prior to connection to any DMS component and that file transfers be logged where technically feasible.

Parameter Value(s):

“prohibit connection of unauthorized USB drives or SD cards to DMS controller interfaces; permit use only during approved maintenance activities and require malware scanning prior to connection.”

Standards:

FIPS 140-3⁽⁸⁾, NIST SP 800-56⁽³³⁾, NIST SP 800-171⁽³²⁾, ISO/IEC 27002⁽³¹⁾

AC-21, Information Sharing

Responsible Party (M/I): I

Justification to Select: Threat event "Mishandling of critical and/or sensitive information by authorized users" in table 3Table 5.

Guidance: The IOO establishes procedures to ensure that system logs, configuration data, diagnostic reports, and other security-relevant information are reviewed prior to release and shared only with authorized parties for defined operational, maintenance, or incident response purposes.

Parameter Value(s):

paragraph a. “when sharing system logs, configuration data, firmware information, or diagnostic reports containing security-relevant information with authorized internal departments or external entities such as vendors or contractors.”

paragraph b. “documented review procedures and role-based access controls within the DMS control software to restrict export or sharing of security-relevant information.”

Risk References and Resources

ATT&CK for ICS Mitigations / Techniques:

- M0809 / T0882

AC-24, Access Control Decisions

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Inadequate access controls applied” in table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: The IOO defines the authorization rules, role definitions, and access conditions that govern actions within the DMS control environment. The IOO identifies which system components require enforcement of access control decisions, including message control functions, configuration management interfaces, user management functions, and remote access services.

The manufacturer implements mechanisms within the DMS control software and controller interfaces that enforce access control decisions based on authenticated user identity, assigned role, and defined privileges. The system validates authorization prior to permitting execution of controlled functions.

Parameter Value(s):

#1 “implement mechanisms within the DMS control software to enforce defined authorization rules.”

#2 “user authentication, role-based authorization, and privilege validation prior to execution of controlled functions.”

AT Family – Awareness and Training

AT-3, Role-Based Training

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Inadequate ITS security training and awareness program” in table 6, Policy and Procedure Vulnerabilities and Predisposing Conditions.

Guidance: The IOO establishes and implements role-based cybersecurity training for personnel with responsibilities related to the DMS control environment, including administrators, operators, field technicians, engineers, and supervisory personnel. The training addresses secure operation of the DMS control software, protection of credentials, secure configuration practices, remote access procedures, incident reporting requirements, and handling of security-relevant information.

The IOO ensures that personnel understand their specific responsibilities for protecting message integrity, maintaining system availability, and reporting suspected cybersecurity events.

Manufacturers and integrators ensure that personnel involved in the development, configuration, deployment, or maintenance of DMS devices receive training appropriate to their roles, including

secure development practices, configuration management, vulnerability handling, and secure update procedures relevant to DMS platforms.

Parameter Value(s):

paragraph a. "DMS manufacturers, integrators, administrators, operators, field technicians, and network or security engineers with responsibilities for the DMS control environment."

paragraph a.1. "annually"

paragraph b. #1: "annually"

paragraph b. #2: "upon identification of new threats, vulnerabilities, or adversary tactics and techniques relevant to DMS operations or the ITS environment."

Risk References and Resources:

ATT&CK for ICS Mitigations / Techniques: M0913 / T0859.

NIST SP 800-82:⁽³⁾ Security training includes initial and periodic review of ITS-specific policies, standard operating procedures, security trends, and vulnerabilities. The ITS security training program is consistent with the requirements of the security awareness and training policy established by the organization. The training may be customized for specific ITS roles, which could include operators, maintainers, engineers, supervisors, and administrators.

AU Family – Audit and Accountability

AU-2, Event Logging

Responsible Party (M/I): M/I

Justification to Select: Vulnerability "Logs not maintained" in table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: The IOO defines the events to be logged within the DMS control environment, including security-relevant and operationally significant events. The manufacturer provides configurable logging capabilities within the DMS control software and controller interfaces to support these requirements.

Parameter Value(s):

paragraph a. "system startup and shutdown; application startup and shutdown; message creation, modification, deployment, and removal; configuration changes; firmware updates; successful and unsuccessful logon attempts; account creation, modification, and deletion; remote access session initiation and termination; changes to security settings; and audit configuration changes." paragraph c. "all events defined in AU-2a"

paragraph e. "at least Quarterly"

Risk References and Resources:

NIST SP 800-82:⁽³⁾ Organizations may want to include relevant ITS events (e.g., alerts, alarms, configuration and status changes, operator actions) in their event logging, which may be designated as audit events.

ATT&CK for ICS Mitigations / Techniques:

- M0947 / T0874, T0864, T0859, T0873, T0830, T0811

Standards: NTCIP 1203.3, Section 3.4.⁽⁵⁾

AU-3, Content of Audit Records

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Logs not maintained” in table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: The IOO defines the information to be included in each audit record. The manufacturer ensures that audit records include, at minimum, event type, date and time, user or process identifier, source of the event where applicable, and outcome of the event.

AU-4, Audit Log Storage Capacity

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Logs not maintained” in table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: This is both an organizational and a technical control. The IOO defines the audit log retention requirements and conveys those to the manufacturer/vendor for design and implementation on the DMS.

Parameter Value(s):

“sufficient storage capacity to retain audit logs for a minimum of 30 days of normal operational activity prior to transfer or overwrite.”

Risk References and Resources:

ARC-IT Mechanisms: As specified in control.

ARC-IT protocol implementation conformance statement: Provides 4 megabytes of audit storage.

AU-4(1), Audit Log Storage Capacity | Transfer to Alternate Storage

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Logs not maintained” in table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: It may be necessary to transfer audit logs from the DMS to a centralized system at the TMC where the auditing function will ingest the logs.

Parameter Value(s):

“at least weekly or more frequently if required to prevent log overwrite.”

Risk References and Resources:

NIST SP 800-82:⁽³⁾ Organizational requirements may require storage of exceptionally large amounts of data, which ITS components may not be able to support directly.

AU-5, Response to Audit Processing Failures

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Logs not maintained” in table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: The IOO defines required actions when audit logging processes fail within the DMS control environment. The IOO identifies personnel to be notified and establishes response procedures to ensure logging capability is restored in a timely manner.

The manufacturer implements mechanisms within the DMS control software to detect audit logging failures, generate alerts, and prevent silent loss of audit capability. The system continues core DMS operations while notifying designated personnel of audit processing failures.

Parameter Value(s):

paragraph a: #1 "Security administrators, Local Device Administrators, Remote Device Administrators" #2 "1 hour"

paragraph b: “generate alert and continue system operation; prevent overwriting of existing audit logs where technically feasible.”

AU-5(1), Response to Audit Processing Failures | Storage Capacity Warning

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Logs not maintained” in table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: This is primarily a technical control, but the IOO conveys to the manufacturer/vendor the time period within which a warning is to be provided and the maximum percentage of audit log storage, so the manufacturer/vendor can design and configure the DMS accordingly.

Parameter Value(s):

#1 “notify administrator when audit storage reaches 80 percent capacity.”

#2 “provide warning at least once prior to storage exhaustion.”

#3 “audit logging failures and storage capacity thresholds.”

AU-5(2), Response to Audit Processing Failures | Real-Time Alerts

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Logs not maintained” in table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: The manufacturer provides configurable alerting mechanisms within the DMS control software to notify administrators of audit logging failures, storage exhaustion, or audit capture malfunctions within the configurable timeframe. The IOO configures the timeframe value.

Parameter Value(s):

1st PV: “5 minutes”

2nd PV: “System Administrator and Security Administrator”

3rd PV: “failure of the audit logging process; failure to generate audit records for defined security-relevant events; audit storage reaching critical capacity threshold; inability to write audit records to storage; inability to transmit audit logs to designated centralized storage; or unauthorized attempts to disable or modify audit logging configuration.”

Risk References and Resources:

NIST SP 800-82:⁽³⁾ Example compensating controls include manual mechanisms or procedures. For devices where audit records cannot be feasibly collected, periodic manual review may be necessary.

ARC-IT Mechanisms:

- Provides an alert within 5 seconds to the device operator for any audit failure.
- Provides an alert within 10 seconds to the device administrator for any audit failure; conditional on connectivity to administrator.

AU-6, Audit Record Review, Analysis, and Reporting

Responsible Party (M/I): I

Justification to Select: Vulnerability “Logs not maintained” in table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: The IOO establishes procedures for periodic review and analysis of audit records generated by the DMS control environment. The IOO identifies which audit events require review, including authentication failures, message modifications, configuration changes, firmware updates, and remote access activity.

Parameter Value(s):

paragraph a.1 "At least quarterly"

paragraph a.2. "Minimally, but not limited to: failed system access attempts, system failures, application failures"

paragraph b. "Administrators"

Risk References and Resources:

NIST SP 800-82:⁽³⁾ Organizational requirements may require storage of exceptionally large amounts of data, which ITS components may not be able to support directly.

ATT&CK for ICS Mitigations / Techniques:

- M0947 / T0874, T0864, T0859, T0873, T0830, T0811

AU-6(4), Audit Record Review, Analysis, and Reporting | Central Review and Analysis

Responsible Party (M/I): I

Justification to Select: Vulnerability “Logs not maintained” in table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: The IOO centralizes the collection and review of audit records from the DMS control software and associated components where technically feasible. The IOO defines procedures for

correlating DMS audit logs with logs from related systems or network devices to improve detection of anomalous activity. Centralized review mechanisms support oversight of remote access sessions, configuration changes, and other security-relevant events.

AU-6(6), Audit Record Review, Analysis, and Reporting | Correlation with Physical Monitoring

Responsible Party (M/I): M/I

Justification to Select: Vulnerability "Logs not maintained" in table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: The IOO defines requirements for correlating logical audit records with physical access monitoring events where such capabilities exist. The manufacturer provides logging support for enclosure access, cabinet intrusion detection, or tamper events where supported by the DMS hardware. The IOO reviews correlated physical and logical events to detect unauthorized physical access that may impact system integrity.

AU-7, Audit Record Reduction and Report Generation

Responsible Party (M/I): M

Justification to Select: Vulnerability "Logs not maintained" in table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: The manufacturer provides capabilities within the DMS control software to filter, search, and generate reports from audit records. The IOO defines reporting requirements, including frequency, report recipients, and criteria for identifying suspicious activity.

AU-9, Protection of Audit Information

Responsible Party (M/I): M/I

Justification to Select: Vulnerability "Logs not maintained" in table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: The IOO restricts access to audit records to authorized administrative or security personnel. The manufacturer implements mechanisms within the DMS control software to protect audit logs from unauthorized modification, deletion, or overwriting. The system enforces role-based access controls for audit log access and records attempts to modify or delete audit data.

Parameter Value(s):

paragraph b. "Local device Administrators, Security Administrators"

Risk and Resources:

ARC-IT Mechanisms: Audit information is to be treated as information for which privileged access is required and protected per control AC-03.

AU-9(2), Protection of Audit Information | Store on Separate Physical Systems or Components

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Logs not maintained” in table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: The manufacturer provides the capability to transfer audit records from the DMS control software to a separate storage system designated by the IOO. The IOO defines the frequency and method for transferring audit logs to centralized or alternate storage to prevent loss of audit data due to local storage limitations.

Parameter Value(s):

“at least weekly”

Risk References and Resources:

ARC-IT Mechanisms: See control AU-09.

AU-9(3), Protection of Audit Information | Cryptographic Protection

Responsible Party (M/I): M

Justification to Select: Vulnerability “Logs not maintained” in table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: The manufacturer implements cryptographic mechanisms to protect audit records from unauthorized modification during storage or transmission where required by organizational policy. Cryptographic protections ensure the integrity of audit records and support detection of tampering.

Risk References and Resources:

ARC-IT Mechanisms: See control AU-09.

Standard: FIPS 197⁽¹⁷⁾

AU-11, Audit Record Retention

Responsible Party (M/I): I

Justification to Select: Threat event “Compromise organizational information systems to facilitate exfiltration of data/information” in table 3, Exploit and Compromise.

Guidance: The IOO defines audit record retention requirements for the DMS control environment in accordance with organizational policy and regulatory obligations.

Parameter Value(s):

“3 Years”

AU-12, Audit Record Generation

Responsible Party (M/I): M

Justification to Select: Vulnerability “Logs not maintained” in table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: The manufacturer implements audit record generation capabilities within the DMS control software and controller interfaces. The system automatically generates audit records for security-

relevant events, including authentication activity, message changes, configuration changes, firmware updates, and administrative actions.

Parameter Value(s):

paragraph a. "all information systems and network components"

paragraph b. "Audit administrator"

Risk References and Resources:

ARC-IT Mechanisms: No specific mechanisms are mandated or prohibited.

AU-12(3), Audit Record Generation | Changes by Authorized Individuals

Responsible Party (M/I): M

Justification to Select: Vulnerability "Logs not maintained" in table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: The manufacturer restricts modification of audit configuration settings to authorized administrative roles within the DMS control software. The system generates audit records for all changes to audit configuration, including enabling, disabling, or modifying logging parameters, and associates those changes with the authenticated user performing the action.

Parameter Value(s):

#1 "Local device administrator, Audit administrator"

Risk References and Resources:

NIST SP 800-82:⁽³⁾ Example compensating controls include employing non-automated mechanisms or procedures.

AU-13, Monitoring for Information Disclosure

Responsible Party (M/I): I

Justification to Select: Vulnerability "Logs not maintained" in table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: The IOO establishes procedures to monitor DMS-related communications and system activity for potential unauthorized disclosure of configuration data, audit records, credentials, or other security-relevant information. The IOO identifies external connections, remote access pathways, and data exchange mechanisms that require monitoring and integrates monitoring results into established incident response processes.

Parameter Value(s):

paragraph a. #1 "publicly accessible websites, vendor security advisories, vulnerability disclosure platforms, and other open-source information sites reasonably likely to report exposure of DMS-related information."

paragraph a. #2 "at least weekly and upon notification of a suspected cybersecurity incident or vendor disclosure."

paragraph b. #1 “System Administrator, Security Administrator, and Incident Response Personnel.”

paragraph b. #2 “initiate the incident response process; assess scope and impact to DMS operations; contain the exposure; notify appropriate internal stakeholders; and coordinate with affected external entities as required.”

AU-14, Session Audit

Responsible Party (M/I): M

Justification to Select: Vulnerability “Logs not maintained” in table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: The manufacturer provides the capability within the DMS control software to audit authenticated user sessions. The system records session initiation, session termination, and security-relevant actions performed during the session, and associates those actions with the authenticated user identity.

Parameter Value(s):

paragraph a. #1 “Security administrators”

AU-16, Cross-Organizational Audit Logging

Responsible Party (M/I): M

Justification to Select: Vulnerability “Logs not maintained” in table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: The manufacturer provides mechanisms that enable secure transmission of DMS audit records to external systems where such integration is implemented. The system preserves event integrity and user identity information during transmission to support traceability across organizational boundaries.

Audit export mechanisms support secure, authenticated communication channels and maintain the integrity of transmitted audit records.

Parameter Value(s):

#1 “secure, authenticated, and encrypted communication channels (e.g., TLS-protected log transfer, secure APIs, or VPN-based log forwarding) and documented information exchange agreements.”

#2 “security-relevant DMS audit records, including authentication events, message creation and modification events, configuration changes, firmware update activity, remote access session activity, and audit configuration changes.”

Standards: NIST SP 800-52⁽²⁹⁾, ISO/IEC 18033-3⁽²⁸⁾

CA Family – Assessment, Authorization, and Monitoring

CA-3, Information Exchange

Responsible Party (M/I): I

Justification to Select: Threat event "Compromise organizational information systems to facilitate exfiltration of data/information" in table 3, Exploit and Compromise.

Guidance: The IOO reviews and authorizes all information exchanges between the DMS control environment and external systems. The IOO documents the purpose, data types exchanged, security requirements, and approval authority for each authorized connection.

The IOO ensures that each interconnection is supported by documented agreements that define security responsibilities, authentication requirements, encryption requirements, and monitoring expectations. Risk acceptance decisions associated with DMS interconnections are formally documented.

Parameter Value(s):

paragraph a. "interconnection security agreements and information exchange agreements that define security controls, data types exchanged, and responsibilities of each party."

paragraph c. "at least annually or upon significant change to the DMS architecture or connected external systems."

Risk References and Resources:

NIST SP 800-82:⁽³⁾ Organizations perform risk-benefit analysis to determine whether an ITS should be connected to other systems. The authorizing official fully understands the organizational information security policies and procedures; the ITS security policies and procedures; the risks to organizational operations and assets, individuals, other organizations, and the Nation Select associated with the connection to other systems; the individuals and organizations that operate and maintain the systems, including maintenance contractors or service providers; and the specific health, safety, and environmental risks associated with a particular interconnection. Connections from the ITS environment to other security zones may cross the authorization boundary such that two different authorizing officials may be required to approve the connection. Decisions to accept risk are documented.

ATT&CK for ICS Mitigations / Techniques:

- M0922 / T0811, T0893, T0873, T0882
- M0941 / T0811, T0893, T0839, T0857, T0882

CA-3(6), Information Exchange | Transfer Authorization

Responsible Party (M/I): I

Justification to Select: Threat event "Compromise organizational information systems to facilitate exfiltration of data/information" in table 3, Exploit and Compromise.

Guidance: The IOO authorizes individuals, roles, and external systems permitted to exchange information with the DMS control environment. The IOO documents approved connection paths, authorized user roles, and permitted data flows for each exchange.

CA-3(7), Information Exchange | Transitive Information Exchanges

Responsible Party (M/I): I

Justification to Select: Threat event "Compromise organizational information systems to facilitate exfiltration of data/information" in table 3, Exploit and Compromise.

Guidance: The IOO identifies and documents transitive information exchanges associated with the DMS control environment, including downstream systems that may receive DMS data indirectly through authorized connections. The IOO evaluates the security posture of connected systems that could introduce risk to the DMS through indirect pathways.

CA-5, Plan of Action and Milestones

Responsible Party (M/I): I

Justification to Select: Vulnerability "Lack of a vulnerability management program" in table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: The IOO develops and maintains a Plan of Action and Milestones (POA&M) for the DMS control environment to document identified security weaknesses, planned remediation actions, responsible parties, and target completion dates.

The IOO uses assessment results, audit findings, vulnerability disclosures, configuration reviews, and incident investigations to identify weaknesses requiring corrective action. The IOO tracks remediation progress and documents risk acceptance decisions when corrective actions cannot be immediately implemented.

Where weaknesses relate to vendor-provided components, the IOO coordinates remediation efforts through contractual mechanisms or maintenance agreements but retains responsibility for tracking risk to the DMS environment.

Parameter Value(s):

"review and update the POA&M at least quarterly and upon identification of new security weaknesses or significant system changes."

Risk References and Resources:

NIST SP 800-82:⁽³⁾ Corrective actions identified in assessments may not be immediately actionable in an ITS environment; therefore, short-term mitigations may be implemented to reduce risk as part of the gap closure plan or plan of action and milestones.

CA-6, Authorization

Responsible Party (M/I): I

Justification to Select: Threat event "Exploit poorly configured or unauthorized information systems exposed to the Internet" in table 3, Exploit and Compromise.

Guidance: The IOO formally authorizes the DMS control environment for operation prior to deployment and ensures that a designated senior official accepts responsibility for residual cybersecurity risk associated with the system.

The authorization decision is based on documented security controls, assessment results, identified weaknesses, and planned remediation actions. The IOO ensures that known risks are evaluated and either mitigated or formally accepted before the DMS is placed into or continues operation.

Parameter Value(s):

paragraph e. "at least annually and upon significant system changes, security incidents, or identification of substantial new vulnerabilities."

CA-7, Continuous Monitoring

Responsible Party (M/I): I

Justification to Select: Vulnerability "Inadequate incident detection & response plan and procedures" in table 6, Policy and Procedure Vulnerabilities and Predisposing Conditions.

Guidance: The IOO establishes and implements a continuous monitoring strategy for the DMS control environment that is commensurate with system risk and operational impact. The monitoring strategy addresses detection of unauthorized access, configuration changes, firmware integrity issues, and other security-relevant events.

The IOO defines which DMS components and communication pathways require monitoring, including remote access interfaces, network connections to external systems, and administrative functions.

Parameter Value(s):

paragraph a. "authentication events; remote access activity; configuration changes; firmware update activity; audit logging failures; network connection status to external systems; and firmware integrity verification results."

paragraph b. #1 "real time for critical security alerts; otherwise at least daily."

paragraph b. #2 "weekly"

paragraph g. #1 "Security Administrator and System Administrator"

paragraph g. #2 "at least weekly."

Risk References and Resources:

NIST SP 800-82:⁽³⁾ Continuous monitoring programs for ITS are designed, documented, and implemented with input from ITS personnel. The organization ensures that continuous monitoring does not interfere with ITS functions. The individual or group designing and conducting the continuous monitoring for the ITS implements a monitoring program that is consistent with the organizational information security policies and procedures, the ITS security policies and procedures, and the specific health, safety, and environmental risks associated with a particular facility and/or process. Continuous monitoring can be automated or manual at a frequency sufficient to support risk-based decisions. For example, the organization may monitor event logs manually on a specified frequency less often for lower-risk, isolated systems than for higher-risk, networked systems.

ATT&CK for ICS Mitigations / Techniques:

- M0814 / T0830, T0878, T0803, T0842, T0846, T0888
- M0926 / T0819, T0842, T0866
- M0930 / T0830, T0800, T0802, T0848, T0848, T0864

CA-7(6), Continuous Monitoring | Automation Support for Monitoring

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Inadequate incident detection & response plan and procedures” in table 6, Policy and Procedure Vulnerabilities and Predisposing Conditions.

Guidance: The IOO identifies automated monitoring capabilities appropriate for the DMS environment based on risk and operational constraints. The manufacturer provides configurable capabilities within the DMS control software to support automated generation and transmission of security-relevant logs and alerts. Automated monitoring support may include log export mechanisms, alert generation for defined security events, configuration integrity verification features,

Parameter Value(s):

“automated generation and export of security-relevant audit logs; alerting for defined security events;

CA-8, Penetration Testing

Responsible Party (M/I): I

Justification to Select: Vulnerability “Lack of a vulnerability management program” in table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions. Pen tests serve as a way to examine whether an IOO's security policies are genuinely effective. Pen tests also identify vulnerabilities in a system and provide awareness of and enhance cybersecurity hygiene.

Guidance: The IOO conducts penetration testing of the DMS control environment to evaluate the effectiveness of implemented security controls and to identify exploitable vulnerabilities. Penetration testing is planned and executed in a manner that does not adversely affect DMS safety, availability, or operational performance. The IOO defines the scope of testing, including network boundaries, remote access pathways, externally exposed services, and administrative interfaces. Where feasible, testing is conducted in a test, staging, replicated, or simulated environment representative of the production DMS environment. When production systems are tested, testing is coordinated with operational staff and scheduled to minimize operational impact.

Parameter Value(s):

#1 “at least every three years or upon significant architectural changes, introduction of new externally accessible services, or major system upgrades.”

#2 “externally accessible components of the DMS control environment, including remote access services, network gateways, and administrative interfaces.”

Risk References and Resources:

NIST SP 800-82:⁽³⁾ Penetration testing is used with care on ITS networks to ensure that ITS functions are not adversely impacted by the testing process. In general, ITS systems are highly

sensitive to timing constraints and have limited resources. Example compensating controls include employing a replicated, virtualized, or simulated system to conduct penetration testing. Remove Production ITS may need to be taken offline before testing can be conducted. If ITS systems are taken offline for testing, tests are scheduled to occur during planned ITS outages whenever possible. If penetration testing is performed on non-ITS networks, extra care is taken to ensure that tests do not propagate into the ITS network.

Standard: NIST SP 800-115⁽²²⁾

CA-9, Internal System Connections

Responsible Party (M/I): I

Justification to Select: Vulnerability “Hardware, firmware, and software not under configuration management” in table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: The IOO defines and documents authorized internal connections within the DMS control environment, including connections between DMS controllers, central management software, network infrastructure devices, and maintenance interfaces. For each authorized internal connection, the IOO documents the purpose, permitted protocols, security requirements, and responsible administrative authority. The IOO reviews internal system connections periodically and removes or reauthorizes connections when system configurations change or when connections are no longer required.

Parameter Value(s):

paragraph a. “DMS controllers, central management software at the TMC, and authorized maintenance interfaces.”

paragraph c. “upon device setup, network reconfiguration, detection of security incidents affecting the connection, or when the connection is no longer operationally required.”

paragraph d. “At least annually”

Risk References and Resources:

NIST SP 800-82:⁽³⁾ Organizations perform risk-benefit analysis to determine whether ITS equipment should be connected to other internal system components and then document those connections. The authorizing official fully understands the potential risks associated with approving individual connections or approving a class of components to be connected. For example, the authorizing official may broadly approve the connection of any sensors limited to 4–20 milliamp communication, while other Select connection types (e.g., serial or Ethernet) require individual approval. Decisions to accept risk are documented.

CM Family – Configuration Management

CM-2, Baseline Configuration

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Hardware, firmware, and software not under configuration management” table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: The manufacturer provides a documented baseline configuration for the DMS control software and controller platform that supports secure deployment. The baseline disables or restricts unnecessary services, accounts, and network interfaces not required for DMS operation.

The IOO establishes and maintains a configuration baseline for deployed DMS systems, including firmware versions, configuration parameters, and enabled services. The IOO verifies baseline integrity following maintenance activities, firmware updates, or configuration changes.

Parameter Value(s):

paragraph b.1. "semi-annual

paragraph b.2. "upon significant system changes, security incidents, or vendor-released critical firmware or software updates."

Standard: NCTIP 1203, Section 2.5.1⁽⁵⁾

CM-3, Configuration Change Control

Responsible Party (M/I): M/I

Justification to Select: Vulnerability "Hardware, firmware, and software not under configuration management" in table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: The IOO establishes a configuration change control process for the DMS control environment that documents proposed changes, approvals, implementation actions, and validation results. All changes to firmware, configuration settings, access controls, and communication parameters are formally tracked.

The manufacturer provides logging and reporting capabilities within the DMS control software to record configuration changes and associate them with authenticated user identities.

Risk References and Resources:

NIST SP 800-82:⁽³⁾ Configuration change control procedures should align with the organization's management of change practices.

CM-4, Impact Analysis

Responsible Party (M/I): I

Justification to Select: Vulnerability "Hardware, firmware, and software not under configuration management" in table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: The IOO performs security and operational impact analyses prior to implementing changes to the DMS control environment. The analysis evaluates potential effects on system integrity, availability, interoperability, and roadway safety.

Risk References and Resources:

NIST SP 800-82:⁽³⁾ The organization considers ITS safety and security interdependencies. ITS security and safety personnel are included in change process management if the change to the system may impact safety or security.

CM-5, Access Restrictions for Change

Responsible Party (M/I): I

Justification to Select: Vulnerability “Hardware, firmware, and software not under configuration management” in table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: The IOO restricts physical and logical access to DMS configuration interfaces, firmware update mechanisms, and administrative functions. Only authorized personnel with defined roles may initiate system changes. The IOO enforces access restrictions through role-based access controls, credential management, and physical protection of controller enclosures and maintenance ports.

Risk References and Resources:

NIST SP 800-82:⁽³⁾ Some ITS devices allow for the configuration and use of mode change switches. Where available, these should be used to prevent unauthorized changes. For example, many PLCs have key switches that allow the device to be placed in a programming mode or a running mode. Those PLCs should be placed in a running or remote mode to prevent unauthorized programming changes, and the key should be removed from the key switch and managed appropriately.

CM-5(4), Access Restrictions for Change | Dual Authorization

Responsible Party (M/I): I

Justification to Select: Vulnerability “Hardware, firmware, and software not under configuration management” in table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: The IOO requires dual authorization for high-risk configuration changes that could significantly impact DMS operation or security. Dual authorization applies to firmware updates, modification of access control settings, enabling remote access pathways, and changes to cryptographic or communication parameters. Routine operational message updates do not require dual authorization unless organizational policy dictates otherwise.

CM-6, Configuration Settings

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Hardware, firmware, and software not under configuration management” in table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: The manufacturer provides configurable security-relevant settings within the DMS control software and controller platform consistent with applicable standards and secure deployment practices. The IOO defines and applies approved configuration settings for deployed systems, including communication parameters, authentication settings, and firmware configuration options.

Parameter Value(s):

paragraph a. “National Transportation Communications for ITS Protocol Connected Transportation Interoperability (NTCIP) 1203”

paragraph c. #1 “controller firmware, controller database parameters, communication settings, and access control configuration.”

paragraph c. #2 “operational and security requirements defined by NTCIP 1203 and organizational policy.”

CM-7, Least Functionality

Responsible Party (M/I): M/I

Justification to Select: Threat event "Conduct attacks using unauthorized ports, protocols and services" in table 3, Conduct an Attack (i.e., direct/coordinate attack tools or activities).

The principle of least functionality specifies that systems are configured to provide only essential capabilities and to prohibit or restrict the use of non-essential functions, such as ports, protocols, and/or services that are not integral to the operation of the system. Implementing least functionality is fundamental security effective practices.

Guidance: The manufacturer designs the DMS platform to provide only essential operational capabilities required for message display, control, and system management. Unnecessary services, ports, protocols, and accounts are disabled or removed by default.

The IOO reviews enabled functions and ensures that only mission-essential capabilities remain active in deployed systems.

Parameter Value(s):

paragraph a. “NTCIP-compliant message display and control functions required for authorized DMS operation, including message management, brightness control, status reporting, and administrative access.”

Risk References and Resources:

NIST SP 800-82:⁽³⁾ The organization implements least functionality by allowing only the specified functions, protocols, and/or services required for ITS operations. For non-routable protocols, such as serial communications, interrupts could be disabled or set points could be made read only except for privileged users to limit functionality. Ports are part of the address space in network protocols and are often associated with specific protocols or functions. For routable protocols, ports can be disabled on many networking devices to limit functionality to the minimum required for operation.

ATT&CK for ICS Mitigations / Techniques:

- M0814 / T0830, T0878, T0803, T0842, T0846, T0888
- M0928 / T0847
- M0942 / T0830, T0807, T0885, T0816, T0866, T0822, T0847

Standards: NTCIP 1203⁽⁵⁾

CM-7(2), Least Functionality | Prevent Program Execution

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Poor configurations are used” in table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: The manufacturer provides mechanisms that prevent execution of unauthorized programs on the DMS platform, including disabling auto-execution from removable media and restricting local program installation. The IOO defines policies governing authorized software use and restricts maintenance procedures to approved tools and firmware images.

Parameter Value(s):

"organization-defined policies, access agreements regarding software program usage and restrictions, rules authorizing the terms and conditions of software program usage"

CM-7(4), Least Functionality | Unauthorized Software – Deny-By-Exception

Responsible Party (M/I): M/I

Justification to Select: Vulnerability "Poor configurations are used" in table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: The IOO defines unauthorized software not permitted to execute on the DMS platform. The manufacturer implements mechanisms that prevent execution of software not explicitly authorized, including during disconnected operations.

Parameter Value(s):

paragraph c. "at least annually or upon software update"

CM-7(5), Least Functionality | Authorized Software – Allow by Exception

Responsible Party (M/I): M/I

Justification to Select: Using an allow-list provides a configuration management method to allow the execution of only authorized software which can decrease the likelihood of malicious software executing on the system.

Guidance: The IOO defines the list of authorized software components permitted to execute on the DMS platform. The manufacturer supports an allow-list or equivalent mechanism that restricts execution to approved operating system components, firmware images, and management applications.

Parameter Value(s):

paragraph a. "operating system components, signed firmware images, DMS management applications, cryptographic libraries, and required network communication services."

paragraph c. "at least annually or upon major software or firmware update."

CM-7(9), Least Functionality | Prohibiting the Use of Unauthorized Hardware

Responsible Party (M/I): M/I

Justification to Select: Vulnerability "Hardware, firmware, and software not under configuration management" in table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: The IOO defines authorized hardware components permitted within the DMS control environment, including controllers, network devices, communication modules, and display hardware. Unauthorized hardware devices are prohibited from connection to DMS systems.

The manufacturer supports hardware configuration controls and interface restrictions to prevent unauthorized peripheral or network device connections where technically feasible.

Parameter Value(s):

paragraph a. “NTCIP-compliant DMS controllers, vendor-approved display modules and pixel boards, authorized communication modules, and network infrastructure devices listed on the agency’s approved products list.”

paragraph c. “at least annually or upon introduction of new hardware components.”

CM-8, System Component Inventory

Responsible Party (M/I): I

Justification to Select: Vulnerability “Lack of inventory management policy” in table 6, Policy and Procedure Vulnerabilities and Predisposing Conditions.

Guidance: The IOO develops and maintains an inventory of DMS system components. The inventory includes hardware devices, firmware versions, software components, communication modules, and network infrastructure elements that support DMS operation. The IOO ensures that each component is uniquely identifiable and traceable to a physical location or logical deployment context. The inventory supports configuration management, vulnerability management, and lifecycle planning.

Parameter Value(s):

paragraph a.5. “unique identifier; device location; firmware version; software version where applicable; network address where applicable; and date of last configuration or firmware update.”

paragraph b. “semi-annually or immediately following component replacement, upgrade, or decommissioning”

CM-8(1), System Component Inventory | Updates During Installation and Removal

Responsible Party (M/I): I

Justification to Select: Vulnerability “Lack of inventory management policy” in table 6, Policy and Procedure Vulnerabilities and Predisposing Conditions.

Guidance: The IOO updates the DMS component inventory upon installation, removal, replacement, or upgrade of system components. Inventory updates occur as part of established maintenance or change management processes to ensure accuracy and prevent untracked assets within the DMS environment.

CM-9, Configuration Management Plan

Responsible Party (M/I): I

Justification to Select: Vulnerability “Hardware, firmware, and software not under configuration management” in table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: The IOO develops, documents, and maintains a configuration management plan for the DMS control environment. The plan defines roles and responsibilities for configuration management,

procedures for baseline maintenance, change control processes, and methods for verifying configuration integrity.

Parameter Value(s):

paragraph d. "System Administrator and/or Security Administrator"

CM-10, Software Usage Restrictions

Responsible Party (M/I): I

Justification to Select: Vulnerability "Hardware, firmware, and software not under configuration management" in table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: The IOO establishes policies governing authorized software use within the DMS control environment. The IOO ensures that only licensed, approved firmware and software components are deployed and that software usage complies with applicable licensing agreements and organizational policy.

The IOO tracks authorized software components and ensures that unsupported or unauthorized software is not introduced into the DMS environment.

CM-11, User-installed Software

Responsible Party (M/I): M/I

Justification to Select: Vulnerability "Hardware, firmware, and software not under configuration management" in table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: The IOO establishes policies governing the installation of software within the DMS control environment and defines which roles are authorized to install firmware or software updates.

The manufacturer provides mechanisms within the DMS platform to restrict software installation to authorized roles and to prevent unauthorized local execution of software. Installation mechanisms support validation of firmware or software authenticity where applicable.

Parameter Value(s):

paragraph a. "policies that restrict installation of firmware, software, and executable code on DMS controllers and management systems to authorized administrative roles and approved maintenance activities."

paragraph b. "role-based access control restricting installation privileges; validation of firmware or software authenticity prior to installation; disabling automatic execution from removable media; and logging of all software or firmware installation events."

paragraph c. "at least annually and upon detection of unauthorized software installation events."

CM-11(2), User-installed Software | Software Installation with Privileged Status

Responsible Party (M/I): M/I

Justification to Select: Vulnerability "Hardware, firmware, and software not under configuration management" in table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: The manufacturer ensures that installation of firmware or software on the DMS platform requires authenticated access with privileged administrative status. The system restricts installation capability to defined administrative roles and records installation events for accountability.

CP Family – Contingency Planning

CP-9, System Backup

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Critical configurations are not stored or backed up” in table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: The IOO establishes procedures for backing up DMS configuration data necessary to restore system functionality following disruption. Backup scope includes controller configuration parameters, firmware versions, communication settings, and audit logs where required by policy.

The manufacturer provides mechanisms that allow export or retrieval of configuration data and audit logs to support backup processes. Backups may be performed centrally from the TMC or through authorized maintenance procedures.

Parameter Value(s):

paragraph a. #1 “DMS controller configuration parameters, firmware images where available, communication settings, and audit logs as defined by organizational policy.”

paragraph a. #2 “weekly and immediately prior to applying firmware or configuration updates”

paragraph b. “At least weekly or as defined in the contingency plan”

paragraph c. “When created, received, updated, or as defined in the contingency plan”

Risk References and Resources:

ATT&CK for ICS Mitigations / Techniques:

- M0953 / T0809, T0813, T0826, T0827, T0831

CP-9(1), System Backup | Testing for Reliability and Integrity

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Critical configurations are not stored or backed up” in table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: The IOO tests DMS backup data to ensure that configuration information can be restored to a functional controller. Testing may be performed using spare hardware, staging environments, or controlled restoration procedures that do not disrupt production operations.

The manufacturer provides capabilities that support restoration of configuration data and verification of firmware authenticity where applicable.

Parameter Value(s):

“at least annually or as defined in the contingency plan.”

Risk References and Resources:

NIST SP 800-82:⁽³⁾ Testing for reliability and integrity increases confidence that the system can be restored after an incident and minimizes the impact associated with downtime and outages. The ability to test backups is often dependent on the resources needed to appropriately represent the environment, such as the availability of spare devices and testing equipment. Testing backup and restoration on ITS is often limited to systems with redundancy or spare equipment. In certain cases, sampling will be limited to those redundant systems. Compensating controls may include alternative methods for testing backups, such as hash or checksum validations.

CP-10, System Recovery and Reconstitution

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Critical configurations are not stored or backed up” in table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: The IOO establishes and documents procedures to restore the DMS control environment to a known operational state following disruption. Recovery procedures address restoration of controller firmware, configuration parameters, communication settings, and connectivity with central management systems.

The manufacturer provides mechanisms to support restoration of firmware and configuration data and to verify system integrity following reconstitution.

Parameter Value(s):

“24 hours”

Risk References and Resources:

NIST SP 800-82:⁽³⁾ Reconstitution of the ITS includes considering whether system state variables should be restored to initial values or the values before disruption (e.g., are valves restored to full open, full closed, or settings prior to disruption). Restoring system state variables may be disruptive to ongoing physical processes (e.g., valves initially closed may adversely affect system cooling).

IA Family – Identification and Authentication

IA-2, Identification and Authentication

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Authentication of users, data or devices is substandard or nonexistent” in table 6, Communication and Network Configuration Vulnerabilities and Predisposing Conditions.

Guidance: The IOO defines identification and authentication requirements for all users who access the DMS controller, whether locally at the cabinet or remotely through a TMC, maintenance laptop, or other backhaul connection. The IOO determines user categories, required authentication strength based on privilege level, and whether different mechanisms apply for local versus remote access. These requirements are reflected in organizational policy and system security documentation.

The manufacturer implements technical capabilities within the DMS control software to uniquely identify each user and authenticate users prior to granting access to system functions. The DMS enforces authentication for both privileged and non-privileged accounts and supports role-based access control consistent with IOO-defined policies. Default credentials must be disabled or changed prior to operational deployment, and shared accounts must not be used for normal system operations.

Risk References and Resources:

NIST SP 800-82:⁽³⁾ The organization implements least functionality by allowing only the specified functions, protocols, and/or services required for ITS operations. For non-routable protocols, such as serial communications, interrupts could be disabled or set points could be made read only except for privileged users to limit functionality. Ports are part of the address space in network protocols and are often associated with specific protocols or functions. For routable protocols, ports can be disabled on many networking devices to limit functionality to the minimum required for operation.

ATT&CK for ICS Mitigations / Techniques:

- M0804 / T0800, T0858, T0885, T0816, T0871, T0838, T0839, T0861, T0843, T0845, T0886, T0857

IA-2(1), Identification and Authentication (Organizational Users) | Multifactor Authentication to Privileged Accounts

Responsible Party (M/I): I

Justification to Select: Vulnerability “Authentication of users, data or devices is substandard or nonexistent” in table 6, Communication and Network Configuration Vulnerabilities and Predisposing Conditions.

Guidance: The IOO requires multifactor authentication for all privileged accounts that perform configuration changes, firmware updates, certificate management, access control modifications, or other security-relevant functions. Multifactor authentication must use at least two distinct authentication factors. Remote privileged access to the DMS, including access via TMC or maintenance connections, must always employ multifactor authentication. For local console access within a physically secured cabinet, physical access controls may serve as one authentication factor when explicitly approved by organizational policy and when remote access is not concurrently enabled.

Risk References and Resources:

NIST SP 800-82:⁽³⁾ As a compensating control, physical access restrictions may sufficiently represent one authentication factor, provided that the system is not remotely accessible.

IA-2(2), Identification and Authentication (Organizational Users) | Multifactor Authentication to Non-Privileged Accounts

Responsible Party (M/I): I

Justification to Select: Vulnerability “Authentication of users, data or devices is substandard or nonexistent” in table 6, Communication and Network Configuration Vulnerabilities and Predisposing Conditions.

Guidance: The IOO determines whether non-privileged users who access DMS management interfaces require multifactor authentication based on system exposure and risk. For systems accessible through routed or external networks, multifactor authentication should be implemented for non-privileged accounts to reduce the likelihood of credential compromise and unauthorized access. Where the DMS operates within a physically secured and logically isolated environment, physical safeguards may satisfy one authentication factor if permitted by organizational policy.

Risk References and Resources:

NIST SP 800-82:⁽³⁾ As a compensating control, physical access restrictions may sufficiently represent one authentication factor, provided that the system is not remotely accessible.

IA-3, Device Identification and Authentication

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Authentication of users, data or devices is substandard or nonexistent” in table 6, Communication and Network Configuration Vulnerabilities and Predisposing Conditions.

Guidance: The IOO defines requirements for authenticating DMS devices and external systems that communicate with the DMS, including identification of trusted certificate authorities, acceptable cryptographic standards, and approved device types. These requirements apply to communications between DMS controllers and TMC systems, gateways, maintenance systems, or other networked components.

The manufacturer implements technical mechanisms that enable devices to be uniquely identified and authenticated before participating in operational communications. Such mechanisms may include mutual authentication using X.509 device certificates, TLS-based authentication for IP communications, IEEE 802.1X where supported, or cryptographic verification of device identity and firmware integrity.

Parameter Value(s):

#1 “All field-deployed DMS controllers and any network-connected sign controller components.”

#2 “local; remote; and network connection”

Risk References and Resources:

NIST SP 800-82:⁽³⁾ ITS devices may not inherently support device authentication. If devices are local to one another, physical security measures that prevent unauthorized communication between devices can be used as compensating controls. For remote communication, additional hardware may be required to meet authentication requirements.

IA-5, Authenticator Management

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Inadequate incorporation of security into architecture and design” in table 6, Architecture and Design Vulnerabilities and Predisposing Conditions.

Guidance: This is both an organizational and a technical control. The IOO manages the authenticators, such as verifying identity for initial authenticator distribution, administrative

procedures, or changing or refreshing authenticators. But the IOO also conveys requirements to the manufacturer/vendor for authenticators, such as authenticator content, authenticator strength of mechanism, changing default authenticators prior to use, or protecting authenticators.

Parameter Value(s):

paragraph f. #1 Every 30 days for all authenticators (NIST SP 800-63B)

paragraph f. #2 Accounts or authenticators are reported as compromised

Risk References and Resources:

ATT&CK for ICS Mitigations / Techniques:

- M0927 / T0812, T0822, T0886, T0859
- M0936 / T0822, T0859

NIST SP 800-82:⁽³⁾ Example compensating controls include physical access control and encapsulating the ITS to provide authentication external to the ITS.

ARC-IT Mechanisms:

- Device should store encrypted hashed passwords in a database (only accessible to privileged users) using a strong encryption algorithm.
- Device should enforce password-related security policy (e.g., frequent change, difference between old and new passwords, length).
- Device should provide a secure mechanism for users to update their password.
- Device should only allow network login attempts over a secure channel.
- Device should require the old password for password reset by a user.
- Device should implement a secure mechanism for “forgot password.”
- Device should be able to store public key infrastructure-based credentials.
- Device should support X.509⁽⁷⁾ certificate chain construction.

Standard: NIST SP 800-63B.⁽²⁾

IA-5(1), Authenticator Management | Password-Based Authentication

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Passwords generation, use, and protection not in accord with policy” in table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: This is both an organizational and a technical control. The IOO, for example, decides whether to allow password authentication (as opposed to other methods) and maintain and update a list of commonly used, expected, or compromised passwords such that when users create or update passwords they can be verified against the list. The IOO should convey to the manufacturer/vendor password-based authentication requirements, such as the need to transmit passwords only over cryptographically protected channels, storing passwords securely, employing automated tools to assist in password selection, and enforcing composition and complexity rules.

Parameter Value(s):

paragraph a. “at least quarterly”

paragraph h. “A case sensitive minimum of 8-character mix of uppercase letters, lower case letters, numbers, and special characters in including at least one of each; modify at least 50% of the characters when new passwords are created.”

Risk References and Resources:

ARC-IT Mechanisms: See control IA-05.

- Stores encrypted hashed password in a database (only accessible to privileged users).
- Enforces password-related security policy.
- Provides a secure mechanism for users to update their password.
- Allows network login attempts over a secure channel.
- Requires old password for password reset by a user.
- Implement a secure mechanism for “forgot password.”

Standard: NIST SP 800-63B.⁽²⁾

IA-5(2), Authenticator Management | Public Key-Based Authentication

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Authentication of users, data or devices is substandard or nonexistent” in table 6, Communication and Network Configuration Vulnerabilities and Predisposing Conditions.

Guidance: The IOO establishes or procures a public key infrastructure (PKI) service that operates in accordance with an approved Certificate Policy (CP) and Certification Practice Statement (CPS). The manufacturer implements DMS capabilities that interoperate with the IOO-designated PKI provider. The DMS supports installation and validation of X.509 certificates, certificate chain construction, secure private key storage, and certificate revocation mechanisms consistent with the IOO’s PKI service.

Risk References and Resources:

ARC-IT Mechanisms: See control IA-05

ARC-IT Protocol Implementation Statements:

- Stores public key infrastructure-based credentials.
- Supports X.509⁽⁷⁾ certificate chain construction.

Standard: NIST SP 800-57 Part 1⁽²¹⁾

IA-6, Authenticator Feedback

Responsible Party (M/I): M

Justification to Select: Threat event “Theft of Operational Information” in table 5, Physical Object Threat Events.

Guidance: The manufacturer ensures that the DMS suppresses or obscures authentication feedback during credential entry so that authentication information cannot be observed by unauthorized individuals. For visual interfaces, entered passwords or PINs must be masked to prevent disclosure to casual observers. Authentication error messages must not reveal whether a username is valid or whether a specific portion of the credential was incorrect.

Risk References and Resources:

NIST SP 800-82:⁽³⁾ This control assumes a visual interface that provides feedback about authentication information during the authentication process. When ITS authentication uses an interface that does not support visual feedback (e.g., protocol-based authentication), this control may be tailored out.

ARC-IT Mechanisms: system should not leak information about valid vs invalid usernames by errors or login processing time.

IA-7, Cryptographic Module Authentication

Responsible Party (M/I): M

Justification to Select: Vulnerability “Authentication of users, data or devices is substandard or nonexistent” in table 6, Communication and Network Configuration Vulnerabilities and Predisposing Conditions.

Guidance The manufacturer ensures that any cryptographic module within the DMS that performs encryption, key storage, or certificate processing enforces authentication prior to granting access to cryptographic services in privileged roles. Access to cryptographic keys, key management functions, and security configuration settings must be restricted to authenticated and authorized roles.

Where cryptographic modules are required to meet federal validation requirements, authentication mechanisms must be consistent with the applicable FIPS 140-3 security level implemented by the module. The module must distinguish between authorized roles and enforce separation of key access based on those roles. Processes executing on the DMS must only be permitted to access cryptographic keys and functions consistent with their assigned privileges.

Risk References and Resources:

ARC-IT Mechanisms:

- The device should distinguish between different keys stored by the cryptographic module and should ensure that different processes on the device have only the appropriate access to only the appropriate keys. See control SC-39 for more discussion.
- cryptographic module in the device should require that operators accessing the module in a privileged role authenticate to the cryptographic module using an approved mechanism. Approved mechanisms are any approved for use with FIPS 140-3 level 2.⁽⁸⁾

Standard: FIPS 140-3⁽⁸⁾

IA-8, Identification and Authentication (Non-Organizational Users)

Responsible Party (M/I): M

Justification to Select: Vulnerability “Authentication of users, data or devices is substandard or nonexistent” in table 6, Communication and Network Configuration Vulnerabilities and Predisposing Conditions.

Guidance: The manufacturer ensures that the DMS uniquely identifies and authenticates non-organizational users prior to granting access to system functions. Non-organizational users include maintenance contractors, vendor personnel, integrators, and other external support entities who are authorized to perform diagnostics, maintenance, configuration changes, firmware updates, or other operational tasks.

Authentication mechanisms for non-organizational users must be equivalent in strength to those required for similarly privileged organizational users. Shared or generic vendor accounts must not be used for routine access unless explicitly approved by policy and supported by compensating controls such as enhanced logging and time-bound access. The system must support revocation or disabling of contractor access when no longer required.

Risk References and Resources:

NIST SP 800-82:⁽³⁾ The ITS Discussion for control IA-2, Identification and Authentication (Organizational Users) is applicable for non-organizational users. That is, in cases where shared accounts are required, compensating controls include providing increased physical security, personnel security, and auditing measures. For certain ITS, the capability for immediate operator interaction is critical. Local emergency actions for ITS are not hampered by identification or authentication requirements. Access to these systems may be restricted by appropriate physical controls.

IA-9, Service Identification and Authentication

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Authentication of users, data or devices is substandard or nonexistent” in table 6, Communication and Network Configuration Vulnerabilities and Predisposing Conditions.

Guidance: The IOO determines which system services require identification and authentication based on their impact to DMS operations and roadway safety. Services that initiate configuration changes, retrieve sensitive operational data, manage firmware, or interact with controller databases must require authenticated service access.

The manufacturer implements mechanisms within the DMS to ensure that system services, applications, and automated processes are uniquely identified and authenticated before accessing protected system resources. This includes service-to-service communication between the DMS controller and TMC systems, gateways, or maintenance tools. Authentication mechanisms may include certificate-based mutual authentication, authenticated APIs, or other cryptographically protected methods consistent with organizational requirements.

Parameter Value(s):

“All service-to-service communications that access controller configuration data, controller databases, firmware management functions, or security-relevant system interfaces.”

Risk References and Resources:

ATT&CK for ICS Mitigations / Techniques:

- M0813 / T0800, T0830, T0858, T0868, T0838, T0839, T0861, T0843, T0845, T0886, T0856, T0857, T0855, T0860 (when wireless is supported)

IA-11, Re-authentication

Responsible Party (M/I): M

Justification to Select: Vulnerability “Authentication of users, data or devices is substandard or nonexistent” in table 6, Communication and Network Configuration Vulnerabilities and Predisposing Conditions.

Guidance: The DMS must require users to re-authenticate following defined periods of inactivity, when authentication tokens expire, or when security-relevant session conditions change. The system must invalidate session tokens after logout or timeout and must prevent reuse of expired or terminated sessions.

Parameter Value(s):

“after 15 minutes of inactivity, when authenticators change, and when credentials change”

IR Family – Incident Response

IR-2, Incident Response Training

Responsible Party (M/I): I

Justification to Select: Vulnerability “Inadequate ITS security training and awareness program” in table 6, Policy and Procedure Vulnerabilities and Predisposing Conditions.

Guidance: The IOO provides incident response training to personnel with DMS operational, maintenance, or security responsibilities. Training covers recognition of abnormal DMS behavior, suspected cyber incidents, communication disruptions, physical tampering indicators, and required reporting procedures. Training is role-based and aligned with the organization’s broader incident response plan.

Parameter Value(s):

paragraph a.1. “30 days”

paragraph a.3. “Quarterly”

paragraph b. #1 “Quarterly” #2 “Changes to system roles, responsibilities, or incident awareness”

IR-3, Incident Response Testing

Responsible Party (M/I): I

Justification to Select: Vulnerability “Inadequate ITS security training and awareness program” in table 6, Policy and Procedure Vulnerabilities and Predisposing Conditions.

Guidance: The IOO tests DMS-related incident response procedures to validate detection, reporting, coordination, and recovery processes. Testing may include tabletop exercises, simulated communication failures, or coordinated exercises involving vendors where appropriate.

Parameter Value(s):

#1 Annually

IR-4, Incident Handling

Responsible Party (M/I): I

Justification to Select: Vulnerability “Inadequate ITS security training and awareness program” in table 6, Policy and Procedure Vulnerabilities and Predisposing Conditions.

Guidance: The IOO implements incident handling procedures for DMS systems consistent with the organizational incident response plan. Procedures address detection, analysis, containment, eradication, recovery, and post-incident review. The IOO coordinates with manufacturers, vendors, and integrators when incidents involve firmware, embedded components, communications infrastructure, or supply chain elements.

Risk References and Resources:

NIST SP 800-82:⁽³⁾ As part of the incident handling capability, the organization coordinates with external vendors, integrators, or suppliers as necessary to ensure that they have the capability to address events that are specific to embedded components and devices.

IR-5, Incident Monitoring

Responsible Party (M/I): I

Justification to Select: Vulnerability “Inadequate ITS security training and awareness program” in table 6, Policy and Procedure Vulnerabilities and Predisposing Conditions.

Guidance: The IOO establishes monitoring processes for DMS systems to identify potential security incidents, including unauthorized access attempts, unexpected configuration changes, communication failures, firmware integrity anomalies, or physical tampering indicators. Monitoring may be performed through centralized log aggregation at the TMC, integration with security information and event management systems, or defined manual review processes.

Risk References and Resources:

ARC-IT Mechanisms:

- The system should support audit log functionality as specified in the AU family of controls.

IR-6, Incident Reporting

Responsible Party (M/I): I

Justification to Select: Vulnerability “Inadequate ITS security training and awareness program” in table 6, Policy and Procedure Vulnerabilities and Predisposing Conditions.

Guidance: The IOO defines internal and external reporting requirements for DMS-related security incidents. Reporting procedures specify timeframes, notification recipients, escalation paths, and

coordination requirements with external entities such as state cybersecurity offices, law enforcement, or federal partners where applicable.

Parameter Value(s):

paragraph a. "At least 24 hours"

paragraph b. "Local administrators", "Security administrators"

Risk References and Resources:

NIST SP 800-82:⁽³⁾ The organization should report incidents on a timely basis. The Cybersecurity and Infrastructure Security Agency collaborates with international and private-sector computer emergency response teams to share control systems-related security incidents and mitigation measures.

MA Family – Maintenance

MA-2, Controlled Maintenance

Responsible Party (M/I): I

Justification to Select: Vulnerability "Hardware, firmware, and software that are not under asset management" in table 6, Policy and Procedure Vulnerabilities and Predisposing Conditions.

Guidance: The IOO establishes and enforces procedures for scheduling, documenting, approving, and reviewing maintenance activities performed on DMS components. Maintenance includes firmware updates, configuration changes, hardware repair, and diagnostic activities performed locally or remotely.

Maintenance activities must be authorized prior to execution and documented in maintenance records. When DMS components are removed for off-site repair, the IOO ensures that sensitive configuration data, credentials, and audit information are protected or sanitized in accordance with organizational policy. Following maintenance, the system must be validated to confirm that security configurations, communication settings, and firmware integrity remain consistent with the approved baseline.

Parameter Value(s):

paragraph c. "Maintenance administrators"

paragraph d. "System security configurations", "Network configurations", "User data", "Audit log data"

paragraph f. "Maintenance date and timestamp", "Impacted components", "System changes", "Hardware changes"

MA-3, Maintenance Tools

Responsible Party (M/I): I

Justification to Select: Vulnerability "Hardware, firmware, and software that are not under asset management" in table 6, Policy and Procedure Vulnerabilities and Predisposing Conditions.

Guidance: The IOO approves and controls maintenance tools used to service DMS components, including diagnostic software, firmware update utilities, and configuration tools. Approved tools must be documented and restricted to authorized personnel. Maintenance tools used to connect locally or remotely to DMS devices must be authenticated and operated over secure communication channels where applicable. Local maintenance interfaces such as USB, serial, or console ports should be disabled by default unless operationally required. When enabled for maintenance, access must be controlled, time-bound, and logged in accordance with organizational policy.

Parameter Value(s):

paragraph b. "annually"

MA-3(6), Maintenance Tools | Software Updates and Patches

Responsible Party (M/I): I

Justification to Select: Vulnerability "Hardware, firmware, and software that are not under asset management" in table 6, Policy and Procedure Vulnerabilities and Predisposing Conditions.

Guidance: The IOO establishes a process for securely applying firmware updates, patches, and software revisions to DMS devices. Updates must be validated for authenticity and integrity prior to installation, such as through digital signature verification or checksum validation consistent with organizational cryptographic policy.

Updates should be tested in a controlled environment or pilot deployment where feasible before broad rollout. Maintenance actions must be documented and coordinated to minimize disruption to operational messaging and roadway safety.

MA-4, Nonlocal Maintenance

Responsible Party (M/I): M/I

Justification to Select: Vulnerability "Hardware, firmware, and software that are not under asset management" in table 6, Policy and Procedure Vulnerabilities and Predisposing Conditions.

Guidance: The IOO defines conditions under which nonlocal (remote) maintenance of DMS components is permitted. Remote maintenance must be explicitly authorized, time-bound, and performed using secure, authenticated communication channels.

The manufacturer ensures that the DMS supports secure remote maintenance capabilities consistent with organizational requirements. Remote sessions must terminate upon completion of maintenance activities or after defined inactivity thresholds. Remote maintenance capabilities must not bypass identification, authentication, or auditing requirements established under IA and AU controls.

MA-4(1), Nonlocal Maintenance | Logging and Review

Responsible Party (M/I): M/I

Justification to Select: Vulnerability "Hardware, firmware, and software that are not under asset management" in table 6, Policy and Procedure Vulnerabilities and Predisposing Conditions.

Guidance: The IOO requires that all remote maintenance sessions involving DMS components generate detailed audit records sufficient to support accountability and forensic review. The manufacturer ensures that the DMS logs remote session initiation, termination, and maintenance

actions. Audit logs must be retained and reviewed in accordance with AU family controls to detect unauthorized or anomalous maintenance activity.

Parameter Value(s):

“All remote maintenance sessions including firmware uploads, configuration changes, NTCIP command execution, session start and end times, source system identity, and authentication results.”

MA-4(4), Nonlocal Maintenance | Authentication and Separation of Maintenance Sessions

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Hardware, firmware, and software that are not under asset management” in table 6, Policy and Procedure Vulnerabilities and Predisposing Conditions.

Guidance: The IOO requires that remote maintenance sessions use replay-resistant authentication mechanisms and be logically or physically separated from general operational traffic where feasible.

Parameter Value(s):

paragraph a. “Mutual TLS 1.3 using X.509 certificates issued by an IOO-approved PKI, with keys stored in hardware-backed cryptographic modules where supported.”

Risk References and Resources:

NIST SP 800-82:⁽³⁾ ITS environments are often heavily dependent on nonlocal maintenance providers, so organizations should have the ability to review logs about relevant maintenance activities.

MA-6, Timely Maintenance

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Hardware, firmware, and software that are not under asset management” in table 6, Policy and Procedure Vulnerabilities and Predisposing Conditions.

Guidance:

The IOO establishes requirements for timely repair and replacement of critical DMS components to minimize operational disruption and roadway safety impact. Contracts and service-level agreements define response times, spare part availability, and escalation procedures. The manufacturer supports these requirements by providing replacement components, firmware updates, and technical support within agreed timeframes.

Parameter Value(s):

#1 “Controllers, display panels, communication modules, and power supply units.”

#2 “Within 4 hours for critical failures affecting operational availability, or as defined in service-level agreements.””

PE Family – Physical and Environmental Protection

PE-2, Physical Access Authorizations

Responsible Party (M/I): I

Justification to Select: Vulnerability “Unauthorized personnel have physical access to equipment” in table 6, Physical Vulnerabilities and Predisposing Conditions.

Guidance: The IOO establishes and maintains physical access authorization procedures for DMS field equipment, including sign controller cabinets and associated enclosures. Because DMS units are roadside assets rather than facility-based systems, physical access is controlled through key management, access credential control, and documented authorization lists. The IOO maintains records identifying individuals authorized to access sign controller cabinets and updates those records when personnel roles change.

Parameter Value(s):

paragraph c. “at least annually”

PE-2(1), Physical Access Authorizations | Access by Position or Role

Responsible Party (M/I): I

Justification to Select: Vulnerability “Unauthorized personnel have physical access to equipment” in table 6, Physical Vulnerabilities and Predisposing Conditions.

Guidance: The IOO grants physical access to DMS controller cabinets based on defined positions or roles, such as installers, field technicians, maintenance personnel, and system administrators. Access privileges are limited to individuals whose job responsibilities require physical interaction with the sign controller or associated components.

PE-3, Physical Access Control

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Unauthorized personnel have physical access to equipment” in table 6, Physical Vulnerabilities and Predisposing Conditions.

Guidance: The IOO controls physical access to DMS sign controller cabinets through key control, credential management, and access authorization procedures. The manufacturer designs DMS enclosures and controller cabinets with physical security features such as lockable doors, reinforced enclosures, and support for tamper detection where required.

Parameter Value(s):

paragraph a. “Sign controller cabinet door and associated enclosure access points.”

paragraph a.2. “near field communication (NFC) locks, integrated keyed lock or external padlock”

paragraph f. #2 “at least annually, or when personnel with access to keys are transferred or terminated”

paragraph g. “at least annually”

Risk References and Resources:

NIST SP 800-82:⁽³⁾ The organization considers ITS safety and security interdependencies. The organization considers access requirements in emergency situations. During an emergency-related event (e.g., police need to control an intersection), the organization may restrict access to authorized individuals only. Physical access controls and defense-in-depth measures are used by the organization when necessary and possible to supplement ITS security when electronic mechanisms (e.g., cabinet alarm when opened) are unable to fulfill the security requirements of the organization's security plan.

PE-3(1), Physical Access Control | System Access

Responsible Party (M/I): I

Justification to Select: Vulnerability "Unauthorized personnel have physical access to equipment" in table 6, Physical Vulnerabilities and Predisposing Conditions.

Guidance: The IOO ensures that physical access to the sign controller is restricted to authorized personnel and that physical access does not bypass logical access controls. The manufacturer ensures that physical access to the cabinet does not automatically grant unrestricted access to system configuration or security functions without proper authentication.

Parameter Value(s):

"The sign controller cabinet and embedded controller interfaces."

PE-3(4), Physical Access Control | Lockable Casings

Responsible Party (M/I): M/I

Justification to Select: Vulnerability "Unauthorized personnel have physical access to equipment" in table 6, Physical Vulnerabilities and Predisposing Conditions.

Guidance: The IOO requires DMS control units and associated electronics to be housed within lockable enclosures. The manufacturer designs controller cabinets and sign housings with lockable casings that protect internal components from unauthorized access.

Parameter Value(s):

"DMS control units and associated electronics"

PE-3(5), Physical Access Control | Tamper Protection

Responsible Party (M/I): M/I

Justification to Select: Threat event "Insert tampered critical components into organizational systems" in table 3, Deliver/Insert/Install Malicious Capabilities.

Guidance: The IOO may require tamper protection or detection mechanisms for critical DMS components based on risk assessment. The manufacturer supports tamper-evident seals, cabinet intrusion detection switches, or protective measures for key components such as the sign controller and communication modules. Tamper controls should detect and alert on unauthorized access; preventive coatings or port disabling mechanisms may be applied where operationally appropriate.

Parameter Value(s):

#1 “Tamper-evident seals, cabinet intrusion detection switches, port covers, or protective enclosures.”

#2 “prevent and detect”

#3 “Critical components including the sign controller and communication modules.”

Risk References and Resources:

ATT&CK for ICS Mitigations / Techniques:

- M0817 / T0862

PE-4, Access Control for Transmission

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Unauthorized personnel have physical access to equipment” in table 6, Section Physical Vulnerabilities and Predisposing Conditions.

Guidance: The IOO identifies physical transmission lines supporting DMS communications and applies protective measures to reduce tampering risk. Protective measures may include conduit protection, locked junction boxes, and restricted access to network termination points.

Parameter Value(s):

#1 “Power and communication lines between the sign controller, sign housing, and backhaul network termination points.”

Risk References and Resources:

ARC-IT Mechanisms:

- The organization shall restrict physical access to all servers and network infrastructure.
- The organization shall implement a Network Access Control system to prevent unauthorized access to corporate networks.

PE-6, Monitoring Physical Access

Responsible Party (M/I): M/I

Justification to Select: Threat “Compromise critical systems via physical access” in table 3, Exploit and Compromise.

Guidance: Because DMS units are deployed in publicly accessible roadside environments, the IOO establishes processes for monitoring physical access events where technically feasible. The manufacturer may support intrusion detection switches, cabinet-open sensors, or environmental alerts that generate events transmitted to the TMC. Monitoring processes should focus on detecting unauthorized cabinet openings, repeated access attempts, or unexplained maintenance activity.

Parameter Value(s):

paragraph b. #1 "at least quarterly"

#2 "unauthorized access attempts, maintenance activities, or physical security incidents"

PE-9, Power Equipment and Cabling

Responsible Party (M/I): M/I

Justification to Select: Threat "Conduct physical attacks on infrastructures supporting organizational facilities" in table 3, Conduct an Attack (i.e., direct/coordinate attack tools or activities).

Guidance: The IOO ensures that external power equipment and cabling supporting the DMS are protected from tampering and environmental damage. The manufacturer designs sign controller housings to protect internal power distribution and communication cabling.

PE-11, Emergency Power

Responsible Party (M/I): M/I

Justification to Select: Threat "Conduct physical attacks on infrastructures supporting organizational facilities" in table 3, Conduct an Attack (i.e., direct/coordinate attack tools or activities).

Guidance: The IOO determines whether emergency or backup power is required for DMS operations based on operational criticality. The manufacturer provides the capability for the DMS to interface with external emergency power sources or internal backup systems where specified. Transition to backup power should occur without requiring manual reconfiguration.

Parameter Value(s):

"Automatic transition to backup power without loss of configuration data."

PE-14, Environmental Controls

Responsible Party (M/I): M/I

Justification to Select: Vulnerability "Loss of environmental control" in table 6, Physical Vulnerabilities and Predisposing Conditions.

Guidance: DMS components are designed to operate in outdoor environments subject to temperature extremes, humidity, precipitation, and other environmental stressors. The IOO defines environmental operating requirements consistent with deployment location. The manufacturer designs the DMS housing and internal components to withstand defined environmental conditions in accordance with applicable standards.

Parameter Value(s):

paragraph b. "continuously"

Risk References and Resources:

NIST SP 800-82:⁽³⁾ ITS can operate in extreme environments and both interior and exterior locations. For a specific ITS, the temperature and humidity design and operational parameters

dictate the performance specifications. As ITS and information technology become interconnected and the network provides connectivity across the hybrid domain, power circuits, distribution closets, routers, and switches that support fire protection and life safety systems must be maintained at the proper temperature and humidity. When environmental controls cannot be implemented, use hardware that is engineered to withstand the unique environmental hazards.

PE-14(2), Environmental Controls | Monitoring with Alarms and Notifications

Responsible Party (M/I): M/I

Justification to Select: Vulnerability "Loss of environmental control" in table 6, Physical Vulnerabilities and Predisposing Conditions.

Guidance: Where environmental monitoring is implemented, the manufacturer provides sensors or diagnostic capabilities to detect overheating, humidity intrusion, or enclosure compromise. The IOO defines which environmental conditions require alerts and establishes notification recipients.

Parameter Value(s):

"Security administrators", Local device administrators, Remote Device administrators"

PE-21, Electromagnetic Pulse Protection

Responsible Party (M/I): M/I

Justification to Select: Vulnerability "Radio frequency, electromagnetic pulse (EMP), static discharge, brownouts, and voltage spikes" in table 6, Physical Vulnerabilities and Predisposing Conditions.

Guidance: The IOO determines whether electromagnetic interference or surge protection measures are required based on risk assessment and deployment environment. The manufacturer designs DMS control units and associated electronics with appropriate surge protection, grounding, and shielding consistent with applicable electrical standards.

Parameter Value(s):

#1 "Surge suppression, grounding, and shielding where required."

#2 "DMS control units and associated electronics"

PL Family – Planning

PL-2, System Security and Privacy Plans

Responsible Party (M/I): I

Justification to Select: Threat "Inadequate organizational ownership of risk assessments" in table 6, Conduct an attack (i.e., direct/coordinate attack tools or activities).

Guidance: A system security plan is necessary at the very minimum in terms of security that an IOO should implement. Reference PL-2 a.7, "Describe any specific threats to the system that are of concern to the organization". The security plan should consider specific threats that targets the key components to the DMS system (e.g., sign controller, field programming terminal, and any exposed connection media).

Parameter Value(s):

paragraph a. "Security administrators, Local Device Administrators, Remote Device Administrators"

paragraph b. "Security administrators, Local Device Administrators, Remote Device Administrators"

paragraph c. "At least Annually"

Risk References and Resources:

NIST SP 800-82:⁽³⁾ When systems are highly interconnected, coordinated planning is essential. A low-impact system could adversely affect a higher-impact system.

PL-7, Concept of Operations

Responsible Party (M/I): M/I

Justification to Select: Vulnerability "Inadequate incorporation of security into architecture and design" in table 6, Architecture and Design Vulnerabilities and Predisposing Conditions.

Guidance: This is primarily an organizational control for the IOO to implement, but the IOO should reach out to the manufacturer if needed for information regarding its concept of operations for the DMS architecture. The IOO should create the concept of operations to describe the intended information security and privacy posture of the DMS throughout its operational lifecycle. This includes how the DMS will manage and protect data in transmission and storage, respond to security incidents, and ensure system availability and integrity during normal operations and under adverse conditions.

Parameter Value(s):

paragraph b. "Annually"

Risk References and Resources:

NIST SP 800-82:⁽³⁾ Organizations need to consider documenting known operational procedures and exploring how they relate to the combination of information technology and ITS technologies within the environment.

PM Family – Program Management

PM-5, System Inventory

Responsible Party (M/I): M/I

Justification to Select: Vulnerability "Lack of a vulnerability management program" in table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: The IOO should develop and maintain a comprehensive inventory of all DMS components, including hardware (e.g., controllers, display panels), software (e.g., software bill of material), and firmware, to ensure accurate tracking and compliance with ITS security requirements. Manufacturers

should provide detailed component specifications and serial numbers to the IOO, ensuring no untracked or unauthorized assets are integrated into the DMS architecture.

Parameter Value(s):

"Quarterly"

PM-9, Risk Management Strategy

Responsible Party (M/I): M/I

Justification to Select: Vulnerability "Lack of a vulnerability management program" in table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: The IOO should establish a risk management strategy for DMS, identifying and prioritizing risks to system availability, integrity, and confidentiality, with mitigation plans integrated into the TMS to ensure uninterrupted traffic messaging. Manufacturers must support the IOO by providing risk assessments for DMS components, including potential vulnerabilities in hardware or firmware, to align with the overall ITS risk management framework.

Parameter Value(s):

"Annually"

Standard: NIST SP 800-37.⁽⁴⁰⁾

PM-30, Supply Chain Risk Management Strategy

Responsible Party (M/I): M/I

Justification to Select: Vulnerability "Lack of a vulnerability management program" in table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: The IOO establishes and maintains a documented supply chain risk management (SCRM) strategy applicable to DMS procurement, deployment, and lifecycle support. The strategy defines how the organization identifies, assesses, and mitigates risks associated with manufacturers, integrators, firmware suppliers, communication module vendors, and other relevant supply chain participants.

The strategy addresses risks such as counterfeit components, malicious code insertion, insecure development practices, inadequate patch support, end-of-life risks, and dependency on third-party services. Supply chain requirements are incorporated into acquisition documents, contracts, and service-level agreements.

Parameter Value(s):

"Annually"

PM-30(1), Supply Chain Risk Management Strategy | Suppliers of Critical or Mission-Essential Items

Responsible Party (M/I): M/I

Justification to Select: Vulnerability "Lack of a vulnerability management program" in table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: The IOO identifies DMS components and services that are considered critical or mission-essential to roadway safety and operational continuity. These may include sign controllers, communication modules, firmware, cryptographic components, remote management services, and any cloud or hosted services supporting DMS operations.

The IOO applies enhanced supply chain risk management requirements to suppliers of those critical components and services. This may include heightened vetting during procurement, contractual security requirements, requirements for vulnerability disclosure programs, lifecycle support commitments, and documentation of secure development and manufacturing practices.

RA Family – Risk Assessment

RA-3, Risk Assessment

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Inadequate organizational ownership of risk assessments” in table 6, Policy and Procedure Vulnerabilities and Predisposing Conditions.

Guidance: This is an organizational control, but the IOO should require the manufacturer/vendor to perform risk assessments to identify relevant threats, vulnerabilities, and potential impacts to the DMS and then design/build in mitigations to reduce the risk during design and development. Once the DMS is delivered, the IOO takes over risk assessments and risk mitigation but may consult the manufacturer/vendor for appropriate risk mitigations. A quantitative risk assessment approach is desirable, but resource constraints and expertise may lead to more qualitative approaches.

Parameter Value(s):

paragraph d “at least annually”

paragraph f. “at least annually”

Standard: NIST SP 800-30.⁽³⁵⁾

RA-3(1), Risk Assessment | Supply Chain Risk Assessment

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Inadequate organizational ownership of risk assessments” in table 6, Policy and Procedure Vulnerabilities and Predisposing Conditions.

Guidance: This is an organizational control, but the IOO should require the manufacturer/vendor to perform supply chain risk assessments to identify potential risks to system components, then select suppliers accordingly and/or design/build in mitigations to reduce the risk in development.

Parameter Value(s):

paragraph a. “system components determined to be key or critical to DMS functions and/or security features (e.g., sign controller)”

paragraph b. “at least annually”

RA-5, Vulnerability Scanning

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Lack of a vulnerability management program” in table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: During development and prior to delivery, the manufacturer performs vulnerability assessments appropriate to the system architecture, including static and dynamic analysis of software, configuration reviews, and testing of exposed services. Identified vulnerabilities are tracked and remediated prior to production release in accordance with defined severity thresholds.

After deployment, the IOO implements vulnerability monitoring and scanning activities consistent with operational risk tolerance. Scanning may include a combination of passive monitoring, configuration reviews, firmware version validation, cross-referencing against public vulnerability databases, and controlled active scanning during planned outages. Automated scanning tools used on adjacent enterprise networks are configured to avoid unintended scanning of field-deployed DMS devices.

All identified vulnerabilities are documented, risk-evaluated, and tracked to remediation or formal risk acceptance.

Parameter Value(s):

paragraph a. “at least every 30 days for vulnerability monitoring activities; active scanning performed in accordance with operational constraints and planned maintenance windows”

Risk References and Resources:

ATT&CK for ICS Mitigations / Techniques:

- M0916 / T0819

NIST SP 800-82:⁽³⁾ The organization makes a risk-based determination of how to monitor or scan for vulnerabilities on their system. This may include active scanning, passive monitoring, or compensating controls, depending on the system being scanned. For example, vulnerability examination may be performed using passive monitoring and manual visual inspection to maintain an up-to-date inventory of assets. That inventory can be cross-referenced against a list of known vulnerabilities (e.g., CISA advisories,⁽⁹⁾ NIST National Vulnerability Database⁽¹⁰⁾). Production may need to be taken offline before active scans can be conducted. Scans are scheduled to occur during planned ITS outages whenever possible. If vulnerability scanning tools are used on adjacent non-ITS networks, extra care is taken to ensure that they do not mistakenly scan the ITS network. Automated network scanning is not applicable to non-routable communications, such as serial networks. Compensating controls include providing a replicated or simulated system for conducting scans or host-based vulnerability applications.

ARC-IT Mechanisms:

- Device scanning to investigate application patch levels, device configuration, exposed services and known vulnerabilities should occur at regular intervals (daily, weekly).
- The device scanning tool will maintain regular security signature updates of its own.
- The device will report on security weaknesses so vulnerabilities can be tracked and remediated centrally.
- Regular network scanning of all connected hosts should occur.
- This could be periodic (monthly) or with any major changes to the network configuration (say the addition of new services or servers).
- Regular network scanning should look for the following:
 - Hosts and services that are exposed but should not be.
 - Known vulnerabilities in exposed services based on public vulnerability databases.
 - Unpatched services that need updating.
 - Weak security configurations (default passwords, lack of authorization controls).
- All exposed web applications/services will undergo regular web application scanning to look for common vulnerabilities affecting web applications (including the OWASP® top 10 vulnerabilities⁽¹¹⁾).
- Any web applications (inaccessible from the public Internet) should undergo a privileged access scan per Control Enhancement 5 to identify issues affecting authenticated users.
- Application source code should undergo regular audits, either periodically or before any major release. This can involve static analysis code audit tools, peer code review, and/or external auditors.
- Regular external audits or penetration tests on the network infrastructure, exposed services, and web applications should be conducted.
- Application binaries should be scanned using a binary analyzer or input fuzzer.
- The organization must have a defined process for tracking all security-related issues and remediation status identified by any scanning or auditing activities.
- The organization should react to all legitimate vulnerabilities.

RA-5(3), Vulnerability Scanning | Breadth and Depth of Coverage

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Lack of a vulnerability management program” in table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: The IOO defines the scope and depth of vulnerability scanning activities to ensure that components with the greatest operational or safety impact receive appropriate coverage. The scope includes field-deployed DMS controllers, communication modules, central management software, supporting servers, and externally exposed services.

Where feasible, scans include authenticated assessment of management interfaces and evaluation of configuration settings, patch levels, exposed services, and known vulnerabilities. Discovered

vulnerabilities are evaluated against authoritative sources, including publicly disclosed vulnerability databases and known exploitable vulnerability catalogs.

RA-7, Risk Response

Responsible Party (M/I): M/I

Justification to Select: Threat “Inadequate organizational ownership of risk assessments” in table 3, Policy and Procedure Vulnerabilities and Predisposing Conditions.

Guidance: The IOO establishes and implements a documented process for responding to identified risks affecting DMS operations. Following risk identification activities (e.g., risk assessments, vulnerability scanning, incident analysis), the IOO determines an appropriate risk response, which may include risk mitigation, risk acceptance, risk avoidance, or risk transfer.

SA Family – System and Services Acquisition

SA-4, Acquisition Process

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Inadequate incorporation of security into architecture and design” in table 6, Architecture and Design Vulnerabilities and Predisposing Conditions.

Guidance: The IOO defines and documents cybersecurity requirements for DMS acquisition and incorporates those requirements into solicitations, contracts, and acceptance criteria. Security requirements address system architecture, authentication, logging, secure communications, configuration management, vulnerability management, supply chain considerations, and lifecycle support.

The IOO ensures that cybersecurity expectations are enforceable through contract language, including requirements for secure development practices, vulnerability disclosure processes, patch support, documentation delivery, and configuration hardening.

Manufacturers implement the agreed-upon cybersecurity requirements throughout system design, development, integration, testing, and delivery. Security features are incorporated into the DMS architecture and verified as part of system acceptance.

Risk References and Resources:

NIST SP 800-82:⁽³⁾ Organizations engage with ITS suppliers to raise awareness of cybersecurity needs. The Supervisory Control and Data Acquisition (SCADA)/Control Systems Procurement Project⁽¹³⁾ provides example cybersecurity procurement language for ITS.

SA-4(5), Acquisition Process | System, Component, and Service Configurations

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Poor configurations are used” in table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: The IOO specifies baseline security configuration requirements in acquisition documentation to ensure DMS components are delivered in a secure default state. These requirements may include disabling unnecessary services, enforcing credential changes prior to operational use, enabling secure communication protocols, and restricting unused ports and interfaces.

Manufacturers deliver DMS components configured in accordance with the approved baseline and provide documentation describing security-relevant configuration settings. Where configuration settings are adjustable by the IOO, recommended secure values are identified in accompanying implementation guidance.

Parameter Value(s):

paragraph a. "Applicable secure configuration baselines, security technical implementation guidance, and documented limitations on functions, ports, protocols, and services"

SA-4(9), Acquisition Process | Functions, Ports, Protocols, and Services in Use

Responsible Party (M/I): M/I

Justification to Select: Threat "Conduct attacks using unauthorized ports, protocols, and services" in table 3, Conduct an Attack (i.e., direct/coordinate attack tools or activities).

Guidance: The IOO defines allowable functions, ports, protocols, and services to be supported by the DMS controller and associated management systems. Requirements include identification of permitted protocol versions, encryption standards, and any restrictions on wireless or remote access services.

SA-5, System Documentation

Responsible Party (M/I): M/I

Justification to Select: Vulnerability "Inadequate incorporation of security into architecture and design" in table 6, Architecture and Design Vulnerabilities and Predisposing Conditions.

Guidance: Manufacturers provide complete and accurate documentation for the DMS controller and associated software applications sufficient to support secure configuration, operation, maintenance, and incident response. Documentation includes system architecture descriptions, interface specifications, supported protocols, configuration guidance, security features, update procedures, and known operational constraints.

The IOO defines documentation requirements in acquisition materials and ensures documentation is reviewed, maintained, and made available to authorized personnel responsible for system administration, security oversight, and operations.

Parameter Value(s):

paragraph d. "system owners, system security officers, system administrators, and any other pertinent personnel or roles"

SA-8, Security and Privacy Engineering Principles

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Inadequate incorporation of security into architecture and design” in table 6, Architecture and Design Vulnerabilities and Predisposing Conditions.

Guidance: The IOO incorporates security and privacy engineering expectations into DMS acquisition requirements to ensure that security is integrated into system architecture and design from inception rather than added after deployment. These expectations are documented in procurement materials and system requirements and are evaluated during design reviews and acceptance testing.

Manufacturers apply recognized security and privacy engineering principles throughout the system development lifecycle, including architecture design, implementation, integration, and testing. Security considerations are embedded into controller firmware, communication interfaces, management applications, and supporting services to reduce attack surface and improve resilience.

Parameter Value(s):

“least privilege, secure defaults, defense in depth, fail securely, complete mediation, separation of duties, and privacy by design

SA-9, External System Services

Responsible Party (M/I): I

Justification to Select: Threat “Conduct attacks using unauthorized ports, protocols, and services” in table 3, Conduct an Attack (i.e., direct/coordinate attack tools or activities).

Guidance: The IOO ensures that contracts or service agreements specify security controls, authentication requirements, encryption standards, vulnerability management expectations, incident notification timelines, and audit rights. The IOO verifies that external service providers implement appropriate protections for DMS-related data and communications and that external connections do not introduce unauthorized functions, ports, protocols, or services into the DMS environment.

The IOO monitors the security posture of external service providers and ensures identified risks are evaluated and addressed in accordance with the organization’s risk management process.

Parameter Value(s):

paragraph a. “multi-factor authentication for administrative access, end-to-end TLS 1.3 encryption for data in transit, signed firmware validation where applicable, and vulnerability scanning in accordance with organizational policy”

paragraph c “annual security posture reporting, automated certificate and firmware signature validation where applicable, annual independent security assessment or penetration testing, and real-time alerting for anomalous or unauthorized traffic affecting DMS communications”

SA-9(2), External System Services | Identification of Functions, Ports, Protocols, and Services

Responsible Party (M/I): I

Justification to Select: Threat “Conduct attacks using unauthorized ports, protocols, and services” in table 3, Conduct an Attack (i.e., direct/coordinate attack tools or activities).

Guidance: The IOO identifies and documents all functions, ports, protocols, and services required for integration between the DMS and any external system services. Only those explicitly authorized functions and communication pathways are permitted.

Parameter Value:

“sign controller, controller database, and any external service interfaces supporting DMS operations”

SA-10, Developer Configuration Management

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Hardware, firmware, and software not under configuration management” in table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: The manufacturer maintains a documented configuration management process for DMS hardware, firmware, software, and supporting documentation across the system lifecycle. Configuration items are uniquely identified, version-controlled, and protected from unauthorized modification. Changes are reviewed, approved, tested, and logged, with traceability to requirements and defect records. The IOO defines configuration visibility and reporting requirements in acquisition materials, including the level of detail needed for tracking security-relevant configuration changes and updates.

Parameter Value(s):

paragraph a. “design, development, implementation, operation, and disposal”

paragraph b. “all configuration items under configuration management”

paragraph c. “CISO, System Administrator, and/or System Owner”

Risk References and Resources:

NIST SP 800-82:⁽³⁾ Personnel knowledgeable in security and privacy requirements are included in the change management process for the developer.

ARC-IT Mechanisms:

- Configuration management changes should be logged and auditable.
- Application developers will use a change management / version control system to ensure that bugs and vulnerabilities do not get reintroduced to the device once they have already been patched.

SA-10(1), Developer Configuration Management | Software and Firmware Integrity

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Hardware, firmware, and software not under configuration management” in table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: The manufacturer implements integrity verification mechanisms for DMS software and firmware, including cryptographic signing of release artifacts and validation of updates prior to installation. The system supports verification of software and firmware against known-good values to detect unauthorized modification.

Risk References and Resources:

NIST SP 800-82:⁽³⁾ Personnel knowledgeable in security and privacy requirements are included in the change management process for the developer.

ARC-IT Mechanisms:

- Configuration management changes should be logged and auditable.
- Application developers will use a change management / version control system to ensure that bugs and vulnerabilities do not get reintroduced to the device once they have already been patched.

SA-10(3), Developer Configuration Management | Hardware Integrity Verification

Responsible Party (M/I): M

Justification to Select: Threat “Conduct supply chain attacks targeting and exploiting critical hardware, software, or firmware” in table 3, Conduct an Attack (i.e., direct/coordinate attack tools or activities). Vulnerability “Hardware, firmware, and software not under configuration management” in table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: The manufacturer implements hardware integrity verification mechanisms appropriate to the DMS architecture. These mechanisms may include secure boot processes, trusted hardware roots of trust, and tamper detection,

Standard: NIST SP 1800-34.⁽¹⁴⁾

SA-11, Developer Security Testing and Evaluation

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Inadequate testing of security changes” in table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: The manufacturer conducts security testing and evaluation activities throughout the DMS development lifecycle to identify and remediate vulnerabilities prior to release. Testing includes functional security testing, integration testing, regression testing, and evaluation of security controls implemented within firmware, controller interfaces, and supporting applications.

The IOO defines security testing expectations in acquisition requirements and may review summary test results, remediation status, or evidence of testing as part of system acceptance.

Parameter Value(s):

paragraph b. #1 "unit, integration, system, and regression"

paragraph b. #2 "at least annually or at each major change to the system"

paragraph b. #3 "full functional coverage for critical components; risk-based sampling for non-critical components"

Risk References and Resources:

ARC-IT Mechanisms:

- Developers should conduct application security penetration testing before any major release.
- Testers should develop a test plan, execute it, and report on findings.

- All flaws identified must be properly documented and either remediated or accepted.

SA-11(2), Developer Security Testing and Evaluation | Threat Modeling and Vulnerability Analyses

Responsible Party (M/I): M

Justification to Select: Vulnerability “Inadequate testing of security changes” in table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: The manufacturer performs structured threat modeling and vulnerability analysis as part of the secure development process for the DMS. Analyses consider system architecture, operational deployment environments, authentication mechanisms, cryptographic boundaries, communication interfaces, and known adversary behaviors.

Threat models and vulnerability analyses are updated for major architectural changes and are reviewed by qualified security personnel. Identified high-severity vulnerabilities are remediated

Parameter Value(s):

paragraph a. "FIPS 199 categorization, operational environment, known/assumed threats from MITRE ATT&CK, and

acceptable risk defined by the IOO's risk management strategy"

paragraph b. "threat modeling, static/dynamic code analysis, vulnerability scanning, and penetration testing"

paragraph c. "high-level for system design, detailed component-level analysis for components affecting authentication or data integrity"

paragraph d. "threat model reviewed and approved by Security Engineer or other authoritative security personnel; all high-severity vulnerabilities remediated or formally accepted"

Standard NIST SP 800-115⁽²²⁾

SA-11(6), Developer Security Testing and Evaluation | Attack Surface Reviews

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Inadequate testing of security changes” in table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: The manufacturer conducts periodic attack surface reviews during development to identify externally reachable interfaces, exposed services, enabled ports, third-party libraries, and other potential entry points. The review verifies alignment with least functionality principles and confirms appropriate authentication, input validation, and protocol hardening.

SA-17, Developer Security and Privacy Architecture and Design

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Inadequate incorporation of security into architecture and design” in table 6, Architecture and Design Vulnerabilities and Predisposing Conditions.

Guidance: The manufacturer defines and documents the DMS security architecture during system design. The architecture describes trust boundaries, privilege separation, cryptographic protections, communication paths, and protective mechanisms for firmware, configuration data, and management interfaces.

SA-17(6), Developer Security and Privacy Architecture and Design | Structured Testing

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Inadequate incorporation of security into architecture and design” in table 6, Architecture and Design Vulnerabilities and Predisposing Conditions.

Guidance: The manufacturer performs structured testing to validate that the implemented security architecture operates as designed under normal, adverse, and stress conditions. Testing includes evaluation of authentication workflows, cryptographic operations, failure modes, and environmental conditions relevant to field deployment. The IOO may require delivery of test summaries or evidence of architectural validation as part of acceptance criteria.

SA-22, Unsupported System Components

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Inadequate incorporation of security into architecture and design” in table 6, Architecture and Design Vulnerabilities and Predisposing Conditions.

Guidance: The IOO maintains awareness of support status for DMS hardware, firmware, and software components and establishes a process to address components that reach end-of-support. Risk associated with unsupported components is evaluated and mitigated through replacement, upgrade, compensating controls, or documented risk acceptance.

Manufacturers provide advance notification of end-of-support timelines, lifecycle policies, and available upgrade paths for DMS components. Where continued use of unsupported components is unavoidable, the IOO documents compensating controls and monitors associated risks.

Parameter Value(s):

paragraph b. “in-house support or support from organization-approved external providers”

Risk References and Resources:

NIST SP 800-82:⁽³⁾ ITS systems may contain system components that are no longer supported by the developer, vendor, or manufacturer and have not been replaced due to various operational, safety, availability, or lifetime constraints. Organizations identify alternative methods to continue supported operation of such system components and consider additional compensating controls to mitigate against known threats and vulnerabilities to unsupported system components.

SC Family – System and Communications Protection

SC-2, Separation of System and User Functionality

Responsible Party (M/I): M

Justification to Select: Allowing non-privileged users to access operating system management functionality capabilities increases the risk that non-privileged users may obtain elevated privileges.

Guidance: The manufacturer designs the DMS to logically separate system management functionality from operational user functionality. Administrative capabilities, including operating system configuration, security settings, firmware management, cryptographic key management, and network configuration, are accessible only to authenticated privileged roles.

Operational user functionality, such as message creation, scheduling, monitoring, and status viewing, is provided through interfaces that do not expose underlying system management features. The system prevents non-privileged users from accessing administrative commands, configuration files, or system-level services.

Risk References and Resources:

NIST SP 800-82:⁽³⁾ Physical separation includes using separate systems for managing the ITS than for operating ITS components. Logical separation includes the use of different user accounts for administrative and operator privileges. Example compensating controls include providing increased auditing measures.

SC-2(1), Separation of System and User Functionality | Interfaces for Non-Privileged Users

Responsible Party (M/I): M

Justification to Select: Allowing non-privileged users to access operating system management functionality capabilities increases the risk that non-privileged users may obtain elevated privileges.

Guidance: The manufacturer provides distinct interfaces for non-privileged operational users that exclude access to system administration functions. Non-privileged users, including operators and maintenance technicians without administrative authority, are prevented from accessing operating system shells, security configuration settings, firmware management utilities, or direct database administration functions.

SC-3, Security Function Isolation

Responsible Party (M/I): M

Justification to Select: Vulnerability “Inadequate incorporation of security into architecture and design” in table 6, Architecture and Design Vulnerabilities and Predisposing Conditions.

Guidance: The manufacturer isolates security functions from non-security application functionality within the DMS architecture. Security-critical processes, including authentication, cryptographic operations, secure communication establishment, and key management, are executed in protected execution contexts separate from message display logic and user-facing application processes.

Risk References and Resources:

NIST SP 800-82:⁽³⁾ Organizations consider implementing this control when designing new architectures or updating existing components. An example compensating control includes access controls.

ARC-IT Mechanisms: The device should separate security functionality from user application functionality by implementing all the following:

- The device requires an authentication mechanism for security functions that is not used for any other function.
- The device requires security functions to use memory that is dedicated exclusively to security functions.

SC-3(1), Security Function Isolation | Hardware Separation

Responsible Party (M/I): M

Justification to Select: Vulnerability “Inadequate incorporation of security into architecture and design” in table 6, Architecture and Design Vulnerabilities and Predisposing Conditions.

Guidance: Where appropriate to the system architecture, the manufacturer implements hardware-based separation mechanisms to protect security functions. These mechanisms may include hardware-enforced memory protection, trusted execution environments, secure boot processes, hardware security modules, or dedicated cryptographic processors.

SC-3(2), Security Function Isolation | Access and Flow Control Functions

Responsible Party (M/I): M

Justification to Select: Vulnerability “Inadequate incorporation of security into architecture and design” in table 6, Architecture and Design Vulnerabilities and Predisposing Conditions.

Guidance: Access control, auditing, and communication flow control functions are implemented in a manner that prevents bypass by application-level processes. These functions operate independently of user applications and enforce authentication, authorization, and secure communications consistently across all interfaces.

SC-3(3), Security Function Isolation | Minimize Non-Security Functionality

Responsible Party (M/I): M

Justification to Select: Vulnerability “Inadequate incorporation of security into architecture and design” in table 6, Architecture and Design Vulnerabilities and Predisposing Conditions.

Guidance: The manufacturer designs the DMS to minimize non-security functionality within security-critical components. Security modules are limited to functions necessary for authentication, cryptography, access control enforcement, and audit generation. Unnecessary services, diagnostic features, or development utilities are excluded from security-critical execution environments.

SC-5, Denial-of-Service Protection

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Denial-of-Service (DoS)” in table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: The manufacturer implements device-level protections within the DMS architecture to resist or limit the effects of resource exhaustion, malformed traffic, excessive management requests, and other disruptive conditions. These protections are designed to preserve safe operation of the sign and prevent unintended message behavior during degraded conditions.

Because DMS devices are typically deployed behind upstream network infrastructure, denial-of-service protection is implemented as a layered approach. Network firewalls, routers, and monitoring systems adjacent to the DMS provide boundary filtering, traffic shaping, and connection management to reduce exposure. The DMS itself enforces internal rate controls, session limits, and safe-state handling where resource exhaustion occurs.

Parameter Value(s):

paragraph a. #1 "Protect"

#2 "network flooding, jamming of wireless communication channels, power disruption, excessive message traffic to DMS controller"

paragraph b. "rate limiting on management interfaces; prioritization of safety-critical message display functions; automatic transition to a predefined safe state upon resource exhaustion; and stateful inspection or connection tracking at network boundaries"

Risk References and Resources:

NIST SP 800-82:⁽³⁾ Some ITS equipment may be more susceptible to DoS attacks due to the criticality of some ITS applications. Risk-based analysis informs prioritization of DoS protection and establishment of policy and procedure.

SC-5(1), Denial-of-Service Protection | Restrict Ability to Attack Other Systems

Responsible Party (M/I): M

Justification to Select: Vulnerability "Denial-of-Service (DoS)" in table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: The manufacturer ensures that the DMS cannot be used as a platform to launch denial-of-service or other disruptive attacks against external systems. The device restricts outbound traffic to only authorized destinations and approved protocols and prevents spoofed or broadcast amplification behavior.

Parameter Value(s):

"network flooding attacks (e.g., TCP SYN floods, UDP floods); broadcast amplification attacks (e.g., Smurf-type amplification); malformed or protocol abuse attacks targeting NTCIP or management interfaces; spoofed source address attacks; and excessive outbound message transmission intended to overwhelm connected TMC or field devices."

SC-5(2), Denial-of-Service Protection | Capacity, Bandwidth, and Redundancy

Responsible Party (M/I): M

Justification to Select: Vulnerability "Denial-of-Service (DoS)" in table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: The manufacturer designs the DMS to maintain operational availability under anticipated peak and abnormal traffic conditions. Network interfaces, processing capacity, and memory resources are appropriately sized to support expected operational loads with additional margin to reduce susceptibility to resource exhaustion.

The architecture includes safeguards such as connection limits, input buffering thresholds, and resource allocation controls to prevent a single source or interface from consuming disproportionate system capacity. Where appropriate, redundancy or upstream network protections may supplement device-level protections to preserve communication with the TMC.

SC-5(3), Denial-of-Service Protection | Detection and Monitoring

Responsible Party (M/I): M/I

Justification to Select: Vulnerability "Denial-of-Service (DoS)" in table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: The IOO defines requirements for monitoring indicators of denial-of-service conditions affecting DMS components or supporting infrastructure. Monitoring requirements identify which system resources and communication channels are subject to observation, including controller processing utilization, memory consumption, network traffic patterns, and communication disruptions.

The manufacturer provides logging and telemetry capabilities within the DMS sufficient to support detection of abnormal traffic volumes, repeated failed connection attempts, protocol anomalies, and resource utilization spikes. These capabilities enable integration with TMC-based monitoring systems or intrusion detection mechanisms.

Parameter Value(s):

paragraph a. "TMC-based intrusion detection capabilities with protocol-aware monitoring for NTCIP communications, network traffic anomaly detection, and controller telemetry reporting CPU utilization, memory consumption, and communication error rates"

SC-6, Resource Availability

Responsible Party (M/I): M

Justification to Select: Vulnerability "Denial-of-Service (DoS)" in table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: The manufacturer designs the DMS to ensure that critical operational and security functions remain available during normal and peak load conditions. System architecture allocates sufficient processing capacity, memory, and communication bandwidth to support real-time message display, controller management, logging, and secure communications.

Parameter Value(s):

#1 "processing capacity, memory allocation, and network bandwidth supporting DMS controller operations and secure communications"

#2 "Priority", "Quota"

SC-7, Boundary Protection

Responsible Party (M/I): M/I

Justification to Select: Vulnerability "Firewalls nonexistent or improperly configured" in table 6, Communication and Network Configuration Vulnerabilities and Predisposing Conditions.

DMSs are becoming more advanced and, therefore, often provide connectivity beyond that to/from the TMC. As such, it is necessary to provide boundary protection to ensure only authorized communications are used to perform approved functions. It is not advisable to rely solely on routers external to the DMS, such as at the TMC, regional network boundaries, or other ITS shelter locations, as there may be other connections to the DMS that need to be managed.

Guidance: The IOO establishes and manages logical boundary protections between DMS controllers and external networks, including segmentation between field devices, enterprise systems, and public networks. The manufacturer ensures that the DMS supports boundary protection by providing configurable interface controls, service and port management, protocol restriction capabilities, and the ability to disable unused communication paths.

Parameter Value:

paragraph b. “logically”

Risk References and Resources:

ATT&CK for ICS Mitigations / Techniques:

- M0935 / T0822
- M0937 / T0806, T0868, T0816, T0839, T0861, T0843, T0845, T0886, T0856, T0857, T0855, T0859

SC-7(3), Boundary Protection | Access Points

Responsible Party (M/I): I

Justification to Select: Vulnerability “No security perimeter defined” in table 6, Architecture and Design Vulnerabilities and Predisposing Conditions.

Guidance: The IOO defines, documents, and authorizes all external access points into the managed ITS network supporting DMS operations. The number and location of access points are based on operational necessity and risk tolerance.

Risk References and Resources:

ARC-IT Mechanisms: See SC-7.

SC-7(5), Boundary Protection | Deny by Default — Allow by Exception

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Inadequate security policy for ITS” in table 6, Policy and Procedure Vulnerabilities and Predisposing Conditions.

Guidance: The IOO establishes deny-by-default policies at managed network interfaces.

The manufacturer ensures that the DMS supports enforcement of allow-listed communications by permitting configuration of authorized peers, services, and protocols while blocking all other traffic.

Parameter Value(s):

"at managed interfaces; for all field-deployed DMS controllers and TMC-to-sign communication paths"

Risk References and Resources:

ARC-IT Mechanisms: See SC-7.

SC-7(7), Boundary Protection | Split Tunneling for Remote Devices

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Inadequate security policy for ITS” in table 6, Policy and Procedure Vulnerabilities and Predisposing Conditions.

Guidance: The IOO prohibits split tunneling for remote devices connecting to the managed ITS network supporting DMS operations.

Parameter Value(s):

"Mandated VPN use"

SC-7(14), Boundary Protection | Protect Against Unauthorized Physical Connections

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “No security perimeter defined” in table 6, Architecture and Design Vulnerabilities and Predisposing Conditions.

Guidance: The IOO defines and secures managed physical interface points that support DMS communications.

The manufacturer designs the DMS to limit exposure of communication and maintenance ports, support secure cable routing, and allow disabling or restricting unused physical interfaces.

Parameter Value(s):

"External communication ports"

Standard: IEEE 802.1X⁽³⁷⁾; IEEE 802.3.⁽¹⁵⁾

SC-7(15), Boundary Protection | Networked Privileged Accesses

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Inadequate security policy for ITS” in table 6, Policy and Procedure Vulnerabilities and Predisposing Conditions.

Guidance: The IOO routes networked privileged access to the DMS through dedicated, managed interfaces that enforce centralized authentication, authorization, and logging. The manufacturer ensures the DMS supports secure privileged access through configurable management interfaces and generates audit records for privileged sessions.

SC-7(16), Boundary Protection | Prevent Exposure of Internal Network Information

Responsible Party (M/I): M

Justification to Select: Vulnerability “Perform perimeter network reconnaissance/scanning.” in table 6, Perform Reconnaissance and Gather Information.

Guidance: The IOO defines policies restricting disclosure of internal network addressing and topology information. The manufacturer ensures the DMS does not expose unnecessary internal addressing,

routing, or configuration details through externally accessible interfaces and minimizes protocol responses that could facilitate reconnaissance.

SC-7(18), Boundary Protection | Fail Secure

Responsible Party (M/I): M

Justification to Select: Threat event “Loss of Safety” in table 5, and vulnerability “Firewalls nonexistent or improperly configured” in table 6, Communication and Network Configuration Vulnerabilities and Predisposing Conditions.

Guidance: The manufacturer ensures the DMS enters a secure operating state when boundary-dependent security services or communications fail. When secure management connectivity is unavailable or when the DMS detects loss of integrity for its communications protections, the system restricts externally initiated management actions and rejects unauthorized sessions.

Risk References and Resources:

NIST SP 800-82:⁽³⁾ The organization selects an appropriate failure mode (e.g., permit or block all communications). Rationale: The ability to choose the failure mode for the physical part of the ITS differentiates the ITS from other information technology systems. This choice may be a significant influence in mitigating the impact of a failure.

ARC-IT Mechanisms: See SC-07.

SC-7(19), Boundary Protection | Block Communication from Non-Organizationally Configured Hosts

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Firewalls nonexistent or improperly configured” in table 6, Communication and Network Configuration Vulnerabilities and Predisposing Conditions.

Guidance: The IOO defines authorized hosts permitted to communicate with DMS controllers. The manufacturer ensures the DMS supports enforcement of host allow-lists and, where required, device authentication mechanisms that validate trusted systems prior to application-level access.

Parameter Value(s):

“individual DMS controllers and authorized TMC or maintenance hosts”

SC-7(21), Boundary Protection | Isolation of System Components

Responsible Party (M/I): I

Justification to Select: Vulnerability “Firewalls nonexistent or improperly configured” in table 6, Communication and Network Configuration Vulnerabilities and Predisposing Conditions.

Guidance: The IOO defines segmentation requirements for isolating DMS controllers from other field devices.

Parameter Value(s):

#1. field-deployed DMS controllers and pixel boards

Risk References and Resources:

NIST SP 800-82:⁽³⁾ The organization selects an appropriate failure mode (e.g., permit or block all communications). Rationale: The ability to choose the failure mode for the physical part of the ITS differentiates the ITS from other information technology systems. This choice may be a significant influence in mitigating the impact of a failure.

ARC-IT Mechanisms: See SC-07.

SC-7(28), *Boundary Protection* | *Connections to Public Networks*

Responsible Party (M/I): I

Justification to Select: Vulnerability “Firewalls nonexistent or improperly configured” in table 6, Communication and Network Configuration Vulnerabilities and Predisposing Conditions.

Guidance: The IOO determines whether any DMS components require connection to public networks and documents risk-based approval for such connections.

Direct connections between DMS controllers and public networks are prohibited unless routed through IOO-managed boundary protection devices.

Parameter Value(s):

"all systems"

Risk References and Resources:

NIST SP 800-82:⁽³⁾ Organizations consider the need for a direct connection to a public network for each ITS system, including potential benefits, additional threat vectors, and potential adverse impact specifically relevant to what type of public access that connection introduces. Rationale: Access to ITS should be restricted to individuals required for operation. A connection made from the ITS directly to a public network has limited applicability in ITS environments, but significant potential risk.

SC-8, *Transmission Confidentiality and Integrity*

Responsible Party (M/I): M

Justification to Select: Threat event “Perform network sniffing of exposed networks” in table 3, Perform Reconnaissance and Gather Information.

The control applies to components that transmit or receive information, as communication paths outside the physical protection of a controlled boundary are exposed to the possibility of interception and modification.

Guidance: The DMS transmits and receives information to/from TMC, sign controller, public-facing applications and local maintenance laptops. The DMS should implement the control either in a typical manner if resources permit or in a customized manner to provide equivalent protections. Integrity protection is more important than confidentiality since the impact of information disclosure is low compared to the impact of data spoofing.

The DMS should also cryptographically authenticate all display commands received from the TMC using signed command messages. Commands must include nonces or sequence numbers to prevent replay. Verification failures must result in rejection and alert generation.

Parameter Value(s):

“confidentiality and integrity, by preventing unauthorized disclosure of information and detecting changes to information”

Risk References and Resources:

NIST SP 800-82:⁽³⁾ When transmitting across untrusted network segments, the organization explores all possible cryptographic integrity mechanisms (e.g., digital signature, hash function) to protect confidentiality and integrity of the information. Example compensating controls include physical protections such as a secure conduit (e.g., point-to-point link) between two system components.

ARC-IT Mechanisms: See SC-8

ATT&CK for ICS Mitigations / Techniques:

- M0802 / T0830, T0858, T0868, T0816, T0831, T0832, T0839, T0861, T0843, T0845, T0848, T0856, T0857, T0855, T0860
- M0808 / T0839, T0842, T0857, T0860, T0887

Standards: RFC 8446, TLS v. 1.3.⁽³⁶⁾

SC-8(1), *Transmission Confidentiality and Integrity* | *Cryptographic Protection*

Responsible Party (M/I): M

Justification to Select: Threat events “Perform network sniffing of exposed networks” in table 3, Perform Reconnaissance and Gather Information, and “Obtain sensitive information through network sniffing of external networks” in table 3, Achieve Results (i.e., cause adverse impacts, obtain information).

Guidance: Cryptographic protection is the only feasible means to protect the information in transit, as physical protection is not possible in most ITS environments. DMS controllers shall ensure message integrity and authenticity for all communications with the TMC and field maintenance systems. Integrity mechanisms such as digital signatures or MACs must be implemented to prevent unauthorized message injection or modification. Confidentiality mechanisms (e.g., TLS 1.3 or IPsec) shall be used where backhaul communications traverse public or cellular networks. Clear-text protocols (e.g., Telnet, FTP, HTTP) shall be disabled.

Parameter Value(s):

“Integrity and authenticity of command and message traffic; TLS 1.3 or IPsec for confidentiality when using public networks.”

Standard: FIPS 140-3.⁽⁸⁾

SC-10, Network Disconnect

Responsible Party (M/I): M

Justification to Select: Threat “Denial of Control” in table 5. The control applies to typical and atypical information technology that transmits or receives information. Communication paths that remain established beyond their usefulness unnecessarily expose transmitted information to the possibility of

interception. Physical objects within the scope of this control set transmit or receive information; therefore, the control applies and is implemented on the physical object or possibly the distant end, either in a typical manner if resources permit or in an atypical manner to provide equivalent protections.

Guidance: Applicable for local connections by an operational user who accesses the signal controller, or a user developer who makes changes to the application programming interface. Not applicable for connections to the TMC, to allow for TLS, heartbeat, etc. Ensure the time period for disconnect is sufficiently short given the sensitivity of the information (e.g., shorter timeout periods for communications paths where information with higher sensitivity is exchanged).

Parameter Value(s):

“no more than 15 minutes”

Risk References and Resources:

NIST SP 800-82:⁽³⁾ NOTE: The intent of this control is effectively covered by AC-17 (09) for ITS systems.

ATT&CK for ICS Mitigations / Techniques:

- M0815 / T0814

ARC-IT Mechanisms:

- For TCP/IP ports in any state other than “LISTENING,” the device should de-allocate that TCP/IP port once 15 minutes have passed with no activity on that port.
- User Datagram Protocol (UDP)/IP ports in any state other than “LISTENING,” the device should de-allocate that UDP/IP port once 15 minutes have passed with no activity on that port.

SC-11, Trusted Path

Responsible Party (M/I): M

Justification to Select: Threat events “Perform network sniffing of exposed networks” in table 3, Perform Reconnaissance and Gather Information, and “Obtain sensitive information through network sniffing of external networks” in table 3, Achieve Results (i.e., cause adverse impacts, obtain information).

Guidance: Manufacturers must design DMS systems to provide a logically isolated trusted communications path, using secure protocols to ensure authenticated TMS administrators and maintenance personnel can securely interact with critical security functions like authentication and configuration management.

Parameter Value(s):

paragraph b. “system” or “regression”

SC-13, Cryptographic Protection

Responsible Party (M/I): M

Justification to Select: Threat events “Perform network sniffing of exposed networks” in table 3, Perform Reconnaissance and Gather Information, and “Obtain sensitive information through network sniffing of external networks” in table 3, Achieve Results (i.e., cause adverse impacts, obtain information).

Guidance: The DMS device should support the cryptographic algorithms necessary to set up TLS tunnels with device certificates. The DMS controller shall support cryptographic mechanisms validated under FIPS 140-3 to establish secure channels (e.g., TLS 1.3) and to authenticate signed messages. Devices must use a NIST SP 800-90A-compliant secure random number generator within a FIPS 140-3 module for all key generation. Certificates and trust anchors used to verify signatures from TMC systems shall be securely stored and periodically updated.

Parameter Value(s):

paragraph a. "confidentiality and integrity of NTCIP 1203 command and control traffic between TMC and field controllers; authentication of controller identity; firmware update integrity"

paragraph b. "TLS 1.3 with mutual certificate-based authentication using ECDSA P-256 and AES-256-GCM for command traffic; X.509 certificates issued by agency PKI with hardware-bound private keys in TPM"

Risk References and Resources:

ARC-IT Mechanisms:

- Devices may support additional cryptographic algorithms.
- Devices should provide a FIPS 140-3⁽⁸⁾ compliant random number generator (i.e., compliant to NIST SP 800-90A Revision 1⁽¹⁶⁾).

Standards: FIPS 140-3,⁽⁸⁾ NIST SP 800-90A Rev. 1.⁽¹⁶⁾

SC-17, Public Key Infrastructure Certificates

Responsible Party (M/I): M/I

Justification to Select: Threat event “Craft counterfeit certificates” in table 3, Craft or Create Attack Tools.

Guidance DMS devices shall be securely provisioned with digital certificates used for authentication, integrity protection, and command authorization between the TMC and field equipment. Certificates may be issued by a trusted external or regional Certificate Authority (CA) under a DOT-approved certificate policy; the TMC may also act as a proxy for certificate provisioning and renewal. Each DMS must be capable of generating its own key pair and submitting a certificate signing request (CSR) to the authorized CA using mutual TLS authentication.

All private keys shall be stored within FIPS 140-3 validated secure elements or TPMs and must never be exportable. Certificates and keys shall be renewed at least every three years, or immediately following firmware replacement, third-party maintenance, or suspected compromise. DMS devices shall support automated re-enrollment and revocation checking using mutual authentication with the TMC CA or SCMS Manager.

Parameter Value(s):

paragraph a “Approved X.509 based certificate policy”

Standards: X.509⁽⁷⁾

SC-23, Session Authenticity

Responsible Party (M/I): M

Justification to Select: Multiple threats in table 3, Conduct an Attack (i.e., direct/coordinate attack tools or activities).

Guidance: The DMS sets up TLS sessions with the TMC and the roadside unit if connected. As such, these are protected with standard TLS security. Any other session level protocols running should also make use of the latest security controls for that protocol (e.g., secure shell equivalents).

Risk References and Resources:

ATT&CK for ICS Mitigations / Techniques:

- M0802 / T0830, T0858, T0868, T0816, T0831, T0832, T0839, T0843, T0845, T0856, T0857, T0855

NIST SP 800-82:⁽³⁾ Example compensating controls include auditing measures.

ARC-IT Mechanisms:

- Approved mechanisms for session authenticity are TLS and Internet Protocol Security (IPSec) with the following parameters, which must be periodically reviewed as algorithms “age” over time and key size recommendations are updated:
 - TLS 1.2 or preferably 1.3 using algorithms currently approved by NIST, with key sizes appropriate for this use.
 - IPSec using algorithms based on the Advanced Encryption Standard⁽¹⁷⁾ currently approved by NIST.
- The device should support at least one of these mechanisms.

Standards: RFC 8446.⁽³⁶⁾

SC-23(1), Session Authenticity | Invalidate Session Identifiers at Logout

Responsible Party (M/I): M

Justification to Select: Multiple threats in table 3, Conduct an Attack (i.e., direct/coordinate attack tools or activities).

Guidance: Upon user logout, all session material should be deleted at the DMS, including session identifiers and any derived cryptographic material.

SC-24, Fail in Known State

Responsible Party (M/I): M

Justification to Select: Failing to a known state helps prevent access by unauthorized persons and ensure integrity of the information is maintained.

Guidance: Manufacturers must design DMS systems to fail in a known secure state that prioritizes traffic and pedestrian safety, such as displaying a blank screen or a preconfigured static safety message (e.g., "Caution: System Offline") when failures like power loss or cyberattacks occur.

Parameter Value(s):

"Known secure state"

Risk References and Resources:

NIST SP 800-82:⁽³⁾ The organization selects an appropriate failure state. Preserving ITS state information includes consistency among ITS state variables and the physical state which the ITS represents (communication permitted or blocked, continue operations).

Rationale: As part of the architecture and design of the ITS, the organization selects an appropriate failure state of an ITS in accordance with the function performed by the ITS and the operational environment. The ability to choose the failure mode for the physical part of ITS differentiates ITS systems from other information technology systems. This choice may be a significant influence in mitigating the impact of a failure since it may be disruptive to ongoing physical processes.

SC-28, Protection of Information at Rest

Responsible Party (M/I): M

Justification to Select: Encryption of information in storage (i.e., data-at-rest) protects the confidentiality and integrity of the information.

Guidance: DMS devices shall protect locally stored configuration, diagnostic, and message logs through cryptographic integrity mechanisms and AES-256 encryption where feasible. Keys must be protected within secure elements or TPMs and regenerated upon device commissioning or compromise.

Parameter Value(s):

#1 "Confidentiality & Integrity", #2 "Message Metadata"

Risk References and Resources:

ATT&CK for ICS Mitigations / Techniques:

- M0941 / T0839, T0857

ARC-IT Mechanisms:

- The device should encrypt data on disk if that data is accessed only by entities with periodic privileged access as defined in Notes on Access Control.(18)
- The device may encrypt data on disk if that data is accessed by entities with ongoing privileged access or with no privileges.
- Keys used to encrypt data on disk should be protected by hardware of at least FIPS 140-3 level 2-equivalent security, such that they cannot be used other than by booting the device.(8)

Standards: FIPS 140-3⁽⁸⁾, FIPS 197⁽¹⁷⁾

SC-28(1), Protection of Information at Rest | Cryptographic Protection

Responsible Party (M/I): M

Justification to Select: Encryption of information in storage (i.e., data-at-rest) protects the confidentiality and integrity of the information.

Guidance: Cryptographic protection is the most widely used method for protection of information at rest. For example, DMS data can be integrity protected (e.g., with a signature or a Message Integrity Check value computed with a key at the DMS).

Parameter Value(s):

#1 “all system components and media”

#2 “all information”

Risk References and Resources:

ARC-IT Mechanisms: See SC-28.

SC-28(3), Protection of Information at Rest | Cryptographic Keys

Responsible Party (M/I): M/I

Justification to Select: Encryption of information in storage (i.e., data-at-rest) protects the confidentiality and integrity of the information.

Guidance: DMS may use cryptographic keys to protect stored configuration data, the controller database, or authentication credentials. These keys must be securely stored to prevent unauthorized disclosure or misuse. The manufacturer/vendor must design the DMS to support the chosen method, including integration with hardware security modules or secure enclaves when required, and must document how cryptographic key material is managed and protected throughout the device lifecycle.

Parameter Value(s):

“FIPS 140-3 validated cryptographic module, Trusted Platform Module, HSM or secure element (SE)”

Standards: FIPS 140-3⁽⁸⁾, NIST SP 800-57 Part 1⁽²¹⁾, NIST SP 800-111⁽²⁰⁾, and ISO/IEC 11889-1:2015⁽²⁶⁾ & 19790:2025⁽²⁷⁾

SC-35, External Malicious Code Identification

Responsible Party (M/I): M/I

Justification to Select: Multiple threats in table 3, Conduct an Attack (i.e., direct/coordinate attack tools or activities).

Guidance: Manufacturers must integrate mechanisms into DMS systems to identify and mitigate external malicious code, such as malware introduced via network interfaces or maintenance ports, ensuring real-time traffic messaging remains secure and operational.

SC-39, Process Isolation

Responsible Party (M/I): M

Justification to Select: Vulnerability “Control network services dependent on a non-control network” in table 6, Architecture and Design Vulnerabilities and Predisposing Conditions.

Guidance: Each application running on the DMS should have its own separate code execution and memory. Security functionality should also be separated. See also ARC-IT guidance as it is applicable to the DMS.

Risk References and Resources:

NIST SP 800-82:⁽³⁾ Example compensating controls include partition processes to separate platforms.

ARC-IT Mechanisms:

- Devices should provide a separate address space for each executing process.
- Devices should ensure that access to protected resources, including signing keys, is only granted to processes that have the appropriate permissions per AC-3.
- Devices should provide address space layout randomization, data execution prevention, and application sandboxing.

SC-39(1), Process Isolation | Hardware Separation

Responsible Party (M/I): M

Justification to Select: Vulnerability “Control network services dependent on a non-control network” in table 6, Architecture and Design Vulnerabilities and Predisposing Conditions.

Guidance: Manufacturers must design DMS systems with hardware separation to isolate critical processes, such as message display and communication functions, using dedicated hardware components or memory segmentation to prevent interference from compromised processes.

SC-40, Wireless Link Protection

Responsible Party (M/I): M

Justification to Select: Vulnerability “Inadequate data protection between clients and servers over wireless connection” in table 6, Communication and Network Configuration Vulnerabilities and Predisposing Conditions.

Guidance: DMS are being developed/delivered with wireless capability; both Wi-Fi and cellular are possible. Appropriate security protection for the Wi-Fi link is advised (e.g., Wi-Fi protected access-based). When DMS devices communicate over cellular or other wireless media, communications shall be encrypted and authenticated using IPsec or TLS 1.3 tunnels. SIM-based authentication (e.g., 3GPP Authentication and Key Agreement Protocol (AKA)) must be paired with device certificate validation to prevent rogue base station attacks. Disable unused wireless radios.

Parameter Value(s):

“802.11a/b/g/n/ac”

Standards: IEEE 802.11a/b/g/n/ac⁽³⁸⁾, 3GPP, & LTE-V2X / NR-V2X

SC-41, Port and I/O Device Access

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Inadequate data protection between clients and servers over wireless connection” in table 6, Communication and Network Configuration Vulnerabilities and Predisposing Conditions.

Guidance: In many cases the DMS is delivered with ports that are not used, and so these ports should be closed prior to operation, to reduce the risk that an adversary may get unauthorized access to the DMS via these ports.

Parameter Value(s):

#1 "physically" #2 “All unused physical ports (e.g., UART, I2C, SPI, etc.).”

Risk References and Resources:

NIST SP 800-82:⁽³⁾ ITS functionality is generally defined in advance and does not change often.

SC-43, Usage Restrictions

Responsible Party (M/I): M/I

Justification to Select: Multiple threats in table 3, Conduct an Attack (i.e., direct/coordinate attack tools or activities).

Guidance: The IOO must establish usage restrictions and implementation guidelines for DMS components, such as controllers, communication modules, and maintenance interfaces, to prevent unauthorized use that could disrupt traffic and pedestrian safety, ensuring only approved functions like real-time message updates are permitted. Manufacturers must design DMS systems to enforce these restrictions through access controls and monitoring mechanisms, logging all component usage within the TMS and providing documentation to the IOO for compliance with ITS security standards.

Parameter Value(s):

"External Device Ports", "Main Controller Interface", "Communications Interface"

SI Family – System and Information Integrity

SI-2, Flaw Remediation

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Lack of a vulnerability management program” in table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: System flaws should be remediated as soon as feasible. Once an update is released from the manufacturer/vendor due to a discovered flaw, the IOO should define the time period required to perform software and/or firmware updates. The manufacturer/vendor should also be responsible for flaw remediation (identify, correct, report, test, install, incorporate) and provide timely reports and updates for the products (controller and applications). If the manufacturer cannot immediately provide a software and/or firmware update for a newly discovered flaw, the manufacturer should recommend or provide other mitigations to be employed while the update is being developed.

U.S. Department of Transportation
Office of the Assistant Secretary for Research and Technology
Intelligent Transportation Systems Joint Program Office

Parameter Value(s):

paragraph c. "less than 30 days (NOTE: less than 30 days is ideal but may not be feasible for all IOOs due to resource limitations and the limited impact to DMS if flaws are not remediated immediately.)"

Risk References and Resources:

NIST SP 800-82:⁽³⁾ Flaw remediation, or patching, is a complex process since an IOO may employ operating systems and software maintained by various vendors. ITS operators may also not have the resources or capability to test patches and are dependent on vendors to validate the operability of a patch. Sometimes the organization has no choice but to accept additional risk if no vendor patch is available, patching requires additional time to complete validation/testing, or deployment requires an unacceptable operations shutdown. In these situations, compensating controls should be implemented (e.g., limiting the exposure of the vulnerable system, restricting vulnerable services, implementing virtual patching). Other compensating controls that do not decrease the residual risk but increase the ability to respond may be desirable (e.g., provide a timely response in case of an incident; devise a plan to ensure the ITS can identify the exploitation of the flaw). Testing flaw remediation in an ITS may exceed the organization's available resources.

ATT&CK for ICS Mitigations / Techniques:

- M0951 / T0820, T0890, T0866, T0862, T0857, T864

SI-3, Malicious Code Protection

Responsible Party (M/I): M/I

Justification to Select: Threat "Insert specialized malware into organizational information systems based on system configurations" in table 3, Deliver/Insert/Install Malicious Capabilities.

Vulnerability "Malware protection implemented without sufficient testing" in table 6, Policy and Procedure Vulnerabilities and Predisposing Conditions.

Guidance: All firmware updates must be signed and validated using vendor-issued certificates before installation. The DMS shall verify cryptographic hashes of firmware images and reject any unsigned or mismatched updates. The IOO should maintain a secure distribution process for firmware updates and maintain verification logs.

Parameter Value(s):

paragraph a. signature based

paragraph c.1 #1 "At least weekly."

paragraph c.1 #2 "Endpoints and network entry/exit points".

paragraph c.2 #1 "Block and quarantine malicious code"

paragraph c.2 #2 "Security Admins, System Admins, and any other pertinent personnel or roles"

Risk References and Resources:

NIST SP 800-82:⁽³⁾ The use and deployment of malicious code protection is determined after careful consideration and after verification that it does not adversely impact the operation of the

ITS. Malicious code protection tools should be configured to minimize their potential impact on the ITS (e.g., employ notification rather than quarantine). Example compensating controls include increased traffic monitoring and auditing.

ATT&CK for ICS Mitigations / Techniques:

- M0938 / T0807, T0871, T0849, T0834, T0853
- M0949 / T0864

ARC-IT Mechanisms:

- The device should be configured to only permit installation and execution of signed code by trusted approved sources. See also, CM-07 in this document.
- The device should detect, prevent, and report download and attempted execution of potentially malicious code.
- The device detection technology implemented will maintain frequent updates of malicious code signatures.

SI-3(4), Malicious Code Protection | Updates Only by Privileges Users

Responsible Party (M/I): M/I

Justification to Select: Vulnerability "Malware protection implemented without sufficient testing" in table 6, Policy and Procedure Vulnerabilities and Predisposing Conditions.

Guidance: The IOO defines which roles are authorized to update malicious code protection mechanisms within the DMS environment. The manufacturer ensures that the DMS restricts modification or updating of malicious code protection mechanisms (e.g., signature files) to authenticated users with explicitly assigned privileged roles. The system enforces role-based access controls and prevents non-privileged users from disabling, bypassing, or altering malicious code protection features.

SI-4, System Monitoring

Responsible Party (M/I): M/I

Justification to Select: Vulnerability "Inadequate data protection between clients and servers over wireless connection" in table 6, Communication and Network Configuration Vulnerabilities and Predisposing Conditions.

Guidance: The IOO defines system monitoring requirements for DMS deployments, including which events, conditions, and communication channels require observation and reporting. Monitoring requirements are risk-based and designed to avoid degrading real-time operational performance.

The manufacturer ensures the DMS provides logging, telemetry, and reporting capabilities sufficient to support IOO-defined monitoring.

Parameter Value(s):

paragraph a.1. "Detect intrusion attempts, malware activity, unauthorized configuration changes, anomalous network traffic, and performance degradation"

paragraph b. "Network-based intrusion detection and prevention (IDPS) systems, host-based IDPS, Security Information and Event Management, file-integrity monitoring, anomaly detection, and log review/alerting."

paragraph g. #1 "Security event logs, IDPS alerts, authentication failures, configuration changes, vulnerability scan results, and incident response reports"

paragraph g. #2 "CISO, Security Admins, System Admins, and any other pertinent personnel or roles"

paragraph g. #3 "as needed and daily (automated), weekly (analyst review), and monthly (formal report)"

Risk References and Resources:

NIST SP 800-82:⁽³⁾ The organization ensures that the use of monitoring tools and techniques does not adversely impact the operational performance of the ITS. Example compensating controls include deploying sufficient network, process, and physical monitoring.

ATT&CK for ICS Mitigations / Techniques:

- M0931 / T0830, T0885, T0884, T0867, T0869

ARC-IT Mechanisms:

- Each device shall have adequate endpoint malware detection and reporting system deployed. In most cases a software suite of end point protections will include firewalls, anti-virus and malware detection, endpoint protection, reporting and logging capabilities (among other features). Consider the capabilities when choosing a software suite and take care in ensuring they are all configured securely.
- Data from each device will be sent to a central collection and monitoring system for threat analysis and auditing.
- Associated malware detection systems will maintain regular updates.
- A network intrusion detection system/intrusion prevention system (IDS/IPS) shall be configured to monitor data and detect malicious code signature in transit from all network infrastructure devices including routers, gateways, firewalls, load balancers and switches.
- The IDS/IPS shall be configured to detect abnormalities in network activity compared to normal operation.
- The network will support centralized monitoring of all relevant security data.
- The IDS/IPS shall be updated regularly and tuned to properly report security incidents.
- A defined notification and response policy and procedure shall be in place for relevant personnel to be informed and act on security incidents.
- A system may be in place to automatically notify relevant personnel per defined policy and further escalate notifications if action is not taken within a defined time period.

SI-4(4), System Monitoring | Inbound and Outbound Communications Traffic

Responsible Party (M/I): M/I

Justification to Select: Vulnerability "Inadequate data protection between clients and servers over wireless connection" in table 6, Communication and Network Configuration Vulnerabilities and Predisposing Conditions.

Guidance: The manufacturer ensures the DMS generates sufficient communication logs and telemetry to enable detection of anomalous traffic patterns, repeated failed connection attempts, protocol violations, and unexpected outbound communications. Monitoring may be performed locally or centrally at the TMC, depending on architecture and resource constraints.

Parameter Value(s):

paragraph b. #1 "weekly"

paragraph b. #2 "intrusion attempts, malware activity, unauthorized configuration changes, anomalous network traffic, and performance degradation"

SI-4(7), System Monitoring | Automated Response to Suspicious Events

Responsible Party (M/I): M/I

Justification to Select: Vulnerability "Intrusion detection and prevention software is not installed" in table 6, Policy and Procedure Vulnerabilities and Predisposing Conditions.

Guidance: The IOO defines which suspicious events require automated notification and what minimally disruptive response actions are authorized.

The manufacturer ensures the DMS supports automated alert generation and secure transmission of event data to centralized monitoring or incident response systems. Where appropriate, the DMS may automatically restrict management access, terminate suspicious sessions, or block repeated unauthorized attempts, provided such actions do not impair safety-critical functions.

Parameter Value(s):

paragraph a. "Security administrators, System Administrators"

paragraph b. "generate detailed event report and transmit securely to centralized monitoring or incident response system"

SI-4(14), System Monitoring | Wireless Intrusion Detection

Responsible Party (M/I): M/I

Justification to Select: Vulnerability "Unauthorized wireless access to sensors or final elements" in table 6, Sensor, Final Element, and Asset Management Vulnerabilities and Predisposing Conditions.

Guidance: Where wireless communication is used, the IOO defines requirements for detecting unauthorized wireless access attempts, rogue devices, or anomalous radio-frequency activity near DMS deployments. The manufacturer ensures that DMS controllers supporting wireless connectivity provide mechanisms for detecting unauthorized association attempts, abnormal signal activity, and authentication failures.

SI-7, Software, Firmware, and Information Integrity

Responsible Party (M/I): M/I

Justification to Select: Threat "Compromise information systems or devices used externally and reintroduced into the enterprise" in table 3, Exploit and Compromise.

Threat "Conduct supply chain attacks targeting and exploiting critical hardware, software, or firmware" in table 3, Conduct an Attack (i.e., direct/coordinate attack tools or activities).

Vulnerability "Hardware, firmware, and software not under configuration management" in table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: The DMS implements cryptographic integrity protections for firmware, configuration data, and operational message content to prevent unauthorized modification. Integrity mechanisms use cryptographic hashing and digital signature validation to detect tampering with controller firmware, boot firmware, configuration files, and authorized message data. Integrity verification must not degrade real-time display functionality or interfere with safety-critical operations.

Upon detection of an integrity violation, the DMS logs the event, restricts further management actions, transitions to a known-good operational state where feasible, and reports the event to centralized monitoring systems. Integrity verification data, including stored hash values, public keys, and validation policies, must be protected from unauthorized modification.

Parameter Value(s):

paragraph a. "boot firmware, display controller firmware, controller configuration data, authorized message content"

paragraph b. "log the event, restrict management access, restart into known-good state, report to security administrators."

Risk References and Resources:

ATT&CK for ICS Mitigations / Techniques:

- M0945/T0849, T0821, T0889, T0839, T0843, T0851, T0862, T0857
- M0946/T0839, T0857
- M0947/T0830, T0811, T0874, T0821, T0836, T0889, T0839, T0843, T0851, T0862, T0857, T0864, T0859

NIST SP 800-82:⁽³⁾ The organization determines whether the use of integrity verification applications would adversely impact the operation of the ITS and employs compensating controls (e.g., manual integrity verifications that do not affect performance).

ARC-IT Mechanisms:

- The device should support integrity checks on software, hardware, and information under certain conditions.
 - The device should protect the list of what is checked and under what circumstances from unauthorized modification per IA-02.
 - The device should support the integrity checks specified in NIST SP 800-147⁽²⁴⁾ section 3.1.2 if the device supports a basic input/output system.⁽¹⁹⁾
 - The integrity checks supported by the device should be hardware-based, i.e., they should use cryptographic information stored in hardware such as a cryptographically secure hash value or a public key to be used for verification.

- Approved mechanisms for satisfying secure boot process in enhancements SI-07(09) and SI-07(10).
- Approved mechanisms specific to dealing with integration of detection and response are specified in IR-04, IR-05.
- The device should either shut down or restart on detection of an integrity violation. Different violations may result in different responses (i.e., a device may support restart and shut down and use them in different circumstances).
- The device should notify the device operator of integrity violations.

SI-7(1), Software, Firmware, and Information Integrity | Integrity Checks

Responsible Party (M/I): M/I

Justification to Select: Threat "Compromise information systems or devices used externally and reintroduced into the enterprise" in table 3, Exploit and Compromise.

Guidance: The DMS performs cryptographic integrity checks during defined lifecycle events, including system startup, restart, prior to firmware installation, and following configuration changes. Integrity verification validates protected components against known-good cryptographic values and prevents execution of unauthorized or altered code.

Parameter Value(s):

#1 "boot firmware, display controller firmware, controller configuration files, authorized message libraries"

#2 "at startup, upon restart, prior to firmware installation, and after configuration changes"

Risk References and Resources:

NIST SP 800-82:⁽³⁾ The organization ensures that the use of integrity verification applications does not adversely impact the operational performance of the ITS.

ARC-IT Mechanisms: See SI-07.

SI-7(2), Software, Firmware, and Information Integrity | Automated Notifications of Integrity Violations

Responsible Party (M/I): M/I

Justification to Select: Vulnerability "Hardware, firmware, and software are not under configuration management" in table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: When integrity violations are detected, the DMS generates automated alerts and securely transmits event details to centralized monitoring systems. If connectivity is unavailable, alerts are stored locally in a tamper-resistant manner for later transmission. Integrity violation events are time-stamped and protected from unauthorized deletion or alteration to preserve forensic value and operational awareness.

Parameter Value(s):

"Security Admins, System Admins, and any other pertinent personnel or roles"

Risk References and Resources:

NIST SP 800-82:⁽³⁾ In situations where the organization cannot employ automated tools that provide notification of integrity discrepancies, the organization employs non-automated mechanisms or procedures. Example compensating controls include performing scheduled manual inspections for integrity violations.

ARC-IT Mechanisms: See SI-07.

SI-7(10), Software, Firmware, and Information Integrity | Protection of Boot Firmware

Responsible Party (M/I): M/I

Justification to Select: Threat "Compromise mission-critical information" in table 3, Section *Exploit and compromise*.

Guidance: The DMS enforces a secure boot process that cryptographically verifies boot firmware and executable images prior to execution. Only authenticated and trusted firmware images are permitted to run on the controller. Boot validation mechanisms rely on hardware-protected cryptographic material where supported and prevent execution of unverified firmware.

Risk References and Resources:

ARC-IT Mechanisms: See SI-07.

Standards: NIST SP 800-193⁽²³⁾ & SP 800-147⁽²⁴⁾

SI-10, Information Input Validation

Responsible Party (M/I): M/I

Justification to Select: Threat "Spoofed reporting message" in table 5.

Threat "Compromise mission-critical information" in table 3, Exploit and Compromise.

Guidance: The DMS validates all externally supplied input prior to processing to prevent malformed, malicious, or unauthorized data from affecting controller operation. Input validation mechanisms apply to network communications, web or management interfaces, database interactions, firmware update channels, and any interface capable of receiving operational commands or configuration data.

Validation mechanisms enforce strict protocol conformance, length checks, type enforcement, range validation, and rejection of unexpected or malformed data structures. For NTCIP-based communications, the DMS validates object identifiers, value ranges, message structure, and command sequencing to prevent spoofed reporting messages or unauthorized display manipulation.

Parameter Value(s):

"All network, wireless, management, configuration, firmware update, and controller command inputs, including NTCIP message objects and associated parameters"

Risk References and Resources:

ARC-IT Mechanisms:

- The network stacks that are provided as part of the device platform should include industry standard input validation protocols for network datagrams.
- All applications installed on the device should conduct input validation on inputs received over a network or wireless interface.

SI-16, Memory Protection

Responsible Party (M/I): M/I

Justification to Select: Threat "Cause deterioration/destruction of critical information system components and functions" in table 3, Achieve Results (i.e., cause adverse impacts, obtain information).

Threat "Cause integrity loss by polluting or corrupting critical data." In table 3, Achieve Results (i.e., cause adverse impacts, obtain information).

Guidance: The DMS implements memory protection mechanisms to prevent unauthorized code execution, memory corruption, and data manipulation. The system employs hardware-enforced protections where supported to prevent execution of code in non-executable memory regions and to mitigate memory exploitation techniques.

Memory protection mechanisms include hardware-enforced data execution prevention and address space layout randomization or equivalent protections supported by the controller platform.

Parameter Value(s):

"hardware-enforced data execution prevention and address space layout randomization"

Risk References and Resources:

ATT&CK for ICS Mitigations / Techniques:

- M0950/T0820, T0890, T0866

ARC-IT Mechanisms:

- The device should implement data execution prevention.
- The device may implement address space layout randomization.
- The implementations should be hardware-enforced.

SR Family – Supply Chain Risk Management

SR-2, Supply Chain Risk Management Plan

Responsible Party (M/I): M/I

Justification to Select: Threat "Conduct supply chain attacks targeting and exploiting critical hardware, software, or firmware" in table 3, Conduct an Attack (i.e., direct/coordinate attack tools or activities).

Guidance: The IOO maintains a supply chain risk management plan addressing risks associated with acquisition, integration, and lifecycle support of DMS components. The plan identifies critical hardware, firmware, and software components; defines risk tolerance; and establishes requirements for supplier transparency, traceability, and integrity protection.

The DMS manufacturer maintains a documented supply chain risk management plan covering sourcing, component traceability, secure development practices, firmware protection, and distribution controls. The manufacturer provides this plan to the IOO for review and alignment with organizational risk requirements.

Parameter Value(s):

U.S. Department of Transportation
Office of the Assistant Secretary for Research and Technology
Intelligent Transportation Systems Joint Program Office

paragraph b. “at least annually”

Standard: NIST SP 800-161⁽²⁵⁾

SR-3, Supply Chain Controls and Processes

Responsible Party (M/I): M/I

Justification to Select: Threats “Insert counterfeit or tampered hardware into the supply chain” and “Insert tampered critical components into organizational systems” in table 3, Deliver/Insert/Install Malicious Capabilities.

Guidance: The manufacturer implements supply chain controls and processes to ensure authenticity, integrity, and traceability of DMS hardware, firmware, and critical software components. Controls include supplier vetting, component traceability, secure handling procedures, controlled firmware distribution, and protection against unauthorized modification during production and logistics.

The IOO incorporates supply chain requirements into procurement contracts and verifies that implemented controls align with organizational risk management expectations.

Parameter Value(s):

paragraph a. #1 “boot firmware, display controller firmware, controller hardware assemblies, communication modules, and other key or critical system components”

paragraph a. #2 “Supply chain management personnel responsible for sourcing, purchasing, logistics, and inventory control”

paragraph c. “documented supply chain security plan”

SR-6, Supplier Assessments and Reviews

Responsible Party (M/I): M/I

Justification to Select: Threat “Create and operate false front organizations to inject malicious components into the supply chain” in table 3, Craft or Create Attack Tools.

Guidance: The manufacturer conducts periodic assessments of suppliers providing critical DMS components to verify compliance with security, quality, and integrity requirements. Assessments evaluate supplier secure development practices, component authenticity controls, firmware protection measures, and incident reporting capabilities.

Parameter Value(s):

“at least annually or as necessitated by security events or incidents.”

SR-6(1), Supplier Assessments and Reviews | Testing and Analysis

Responsible Party (M/I): M/I

Justification to Select: Threat “Create and operate false front organizations to inject malicious components into the supply chain” in table 3, Craft or Create Attack Tools.

Guidance: For critical DMS components, the manufacturer performs technical testing and analysis to validate component authenticity and integrity. Testing may include firmware integrity verification,

hardware authenticity validation, secure boot validation, and vulnerability analysis prior to integration into production systems.

Parameter Value(s):

#1 independent third-party testing

SR-9, Tamper Resistance and Detection

Responsible Party (M/I): M/I

Justification to Select: Threats “Insert counterfeit or tampered hardware into the supply chain” and “Insert tampered critical components into organizational systems” in table 3, Deliver/Insert/Install Malicious Capabilities.

Guidance: The DMS incorporates tamper-resistant and tamper-evident mechanisms to protect critical hardware, firmware storage components, and communication interfaces from unauthorized modification. Physical protections may include sealable or lockable enclosures, tamper-evident seals, protected fasteners, intrusion detection switches, and restricted access to internal communication buses and firmware storage devices.

Where supported, the DMS detects enclosure openings or access to protected internal components and generates an event record upon detection. Tamper detection mechanisms must not interfere with normal operation but must provide reliable indication of unauthorized physical access.

The IOO establishes inspection and response procedures for field personnel to identify signs of tampering and to initiate corrective actions, including escalation to centralized monitoring systems, integrity verification checks, or controlled transition to a safe operational state when warranted.

Risk References and Resources:

ATT&CK for ICS Mitigations / Techniques:

- M0947 / T0874, T0839, T0851, T0864

SR-10, Inspection of Systems or Components

Responsible Party (M/I): M/I

Justification to Select: Threats “Insert counterfeit or tampered hardware into the supply chain” and “Insert tampered critical components into organizational systems” in table 3, Deliver/Insert/Install Malicious Capabilities.

Guidance: DMS components are inspected to verify authenticity, integrity, and absence of unauthorized modification prior to deployment and at defined intervals during operational life. Inspections include physical examination of enclosures and seals, verification of component identifiers and serial numbers, confirmation of approved hardware revisions, and cryptographic validation of firmware and configuration integrity where supported.

The manufacturer provides documentation and verification mechanisms necessary to confirm component authenticity and firmware integrity, including approved part lists, hardware revision identifiers, firmware hash values, and secure validation procedures.

Inspection results are documented and retained to support traceability and supply chain assurance.

Parameter Value(s):

#1 "Quarterly"

#2 "sign controller, display panels, communication modules, firmware images, and controller configuration data"

SR-12, Component Disposal

Responsible Party (M/I): I

Justification to Select: Threats "Insert counterfeit or tampered hardware into the supply chain" and "Insert tampered critical components into organizational systems" in table 3, Deliver/Insert/Install Malicious Capabilities.

Guidance: DMS components removed from service are disposed of in a manner that prevents unauthorized recovery, reuse, or reverse engineering of sensitive firmware, configuration data, cryptographic material, or operational information.

Prior to disposal or transfer, storage media and firmware-bearing components are sanitized using approved data destruction or cryptographic erasure methods appropriate to the media type. Where sanitization is not feasible, components are physically destroyed.

Parameter Value(s):

#1 "firmware images, controller configuration data, cryptographic keys, operational logs, and any data stored on persistent media"

#2 "cryptographic erasure, secure overwrite, or physical destruction (e.g., shredding or media destruction)"

Chapter 5. Implementation Considerations

Organizations should consider the following control guidance when implementing specific system capabilities when a system is used to store, process, or transmit ITS information.

CM-5, Access Restrictions for Change

Access to modify DMS firmware, configuration data, message content, or controller parameters must be restricted through both physical and logical controls. Because DMS controllers execute operational commands that directly affect roadside messaging, unauthorized modification can create safety and operational risks. Physical access to controller cabinets and maintenance ports must be restricted using lockable enclosures and controlled key or credential management. Logical access to management interfaces must require strong authentication and encryption. Management protocols must support authenticated sessions and protect configuration updates from interception or tampering. All configuration and firmware changes should be logged and retained centrally for accountability. Firmware images must be version-controlled and cryptographically validated prior to installation. Update activities should be coordinated to avoid operational disruption and to ensure the ability to restore a known-good configuration if needed.

PE-3, Physical Access Control

DMS deployments are typically located in publicly accessible roadside environments, increasing exposure to physical tampering. Physical access protections should focus on securing controller cabinets, communication interfaces, and internal components that store firmware or configuration data. Lockable enclosures, tamper-evident mechanisms, and restricted access to internal ports should be used to limit unauthorized entry. Where feasible, access events may be logged electronically or monitored through intrusion detection mechanisms within the cabinet. Common shared cabinet keys provide limited security and should be supplemented with stronger key management practices or higher-security locking mechanisms. Access credentials must be controlled, periodically validated, and revoked promptly when personnel roles change.

SI-4(14), System Monitoring | Wireless Intrusion Detection

Where wireless communication is used for DMS connectivity, monitoring mechanisms should be implemented to detect unauthorized wireless access, rogue devices, anomalous signal behavior, and suspicious communication patterns. Wireless monitoring may be implemented at the DMS, at supporting communication infrastructure, or centrally at the TMC. Monitoring capabilities should detect unauthorized association attempts, unexpected changes in signal characteristics, repeated authentication failures, or abnormal traffic patterns.

Appendix A. Threats, Vulnerabilities, and Predisposing Conditions

A broad set of adversarial and non-adversarial threat events down selected and tailored from NIST SP 800-30⁽³⁵⁾ that could potentially impact DMS is provided in Table 3 (adversarial) and Table 4 (non-adversarial) below. The properties of DMS may also present unique opportunities to a threat source, specifically addressing how the threat source can manipulate the process of DMS to cause damage or achieve other malicious purposes (e.g., exfiltration of data). Table 5 provides an overview of potential threat events from NIST SP 800-82⁽³⁾ that are more specific to DMS. Threat events listed below focus on the DMS' (to include surveillance cameras and message signs), not the larger system comprised of various types of physical objects and other components. Various threat events may ultimately impact DMS or its mission/operations, either by compromise of the DMS itself or the larger system (e.g., control center). In the case of potential compromise of the larger system, that larger system must implement certain protections to mitigate those risks. Only if the DMS' can implement a protection measure to mitigate the risk will the threat be considered relevant to the DMS itself and, therefore, controls will be selected in this document to mitigate those risks.

Table 3. Adversarial Threat Events

Threat Events	Tactics, Techniques, and Procedures	Description
<i>Perform Reconnaissance and Gather Information</i>	Perform perimeter network reconnaissance/scanning.	Adversary uses commercial or free software to scan organizational perimeters to obtain a better understanding of the information technology infrastructure.
	Perform network sniffing of exposed networks.	Adversary with access to exposed wired or wireless data channels used to transmit information, uses network sniffing to identify components, resources, and protections. DMS systems core communication could be compromised, affecting the C-I-A of the device.
	Perform reconnaissance and surveillance of targeted.	Adversary uses various means (e.g., scanning, physical observation) over time to examine and assess organizations and ascertain points of vulnerability.
<i>Craft or Create Attack Tools</i>	Craft spear phishing attacks.	Adversary employs phishing attacks targeted at high value targets (e.g., senior leaders/executives).

Threat Events	Tactics, Techniques, and Procedures	Description
	Craft attacks specifically based on deployed information technology environment.	Adversary develops attacks (e.g., crafts targeted malware) that take advantage of adversary knowledge of the organizational information technology environment.
	Craft counterfeit certificates.	Adversary counterfeits or compromises a certificate authority, so that malware or connections will appear legitimate.
	Create and operate false front organizations to inject malicious components into the supply chain.	Adversary creates false front organizations with the appearance of legitimate suppliers in the critical lifecycle path that then inject corrupted/malicious system components into the organizational supply chain.
	Install persistent and targeted sniffers on organizational information systems and networks.	Adversary places within internal organizational information systems or networks software designed to (over a continuous period of time) collect (sniff) network traffic.
<i>Deliver/Insert/Install Malicious Capabilities</i>	Deliver known malware to internal organizational information systems.	Adversary uses common delivery mechanisms to install/insert known malware (e.g., malware whose existence is known) into organizational information systems.
	Deliver known malware to internal organizational information systems.	Adversary uses common delivery mechanisms to install/insert known malware (e.g., malware whose existence is known) into organizational information systems.
	Deliver modified malware to internal organizational information systems.	Adversary uses common delivery mechanisms to install/insert known malware (e.g., malware whose existence is known) into organizational information systems.
	Deliver targeted malware for control of internal systems and exfiltration of data.	Adversary uses more sophisticated delivery mechanisms than email (e.g., FTP) to deliver malware and possibly modifications of known malware to gain access to internal organizational information systems.
	Deliver malware by providing removable media.	Adversary installs malware that is specifically designed to take control of internal organizational information systems, identify sensitive information, exfiltrate the information back to adversary, and conceal these actions.

Threat Events	Tactics, Techniques, and Procedures	Description
	Insert untargeted malware into downloadable software and/or into commercial information technology products.	Adversary corrupts or inserts malware into common freeware, shareware, or commercial information technology products. Adversary is not targeting specific organizations, simply looking for entry points into internal organizational information systems. Note that this is particularly a concern for mobile applications.
	Insert targeted malware into organizational information systems and information system components.	Adversary inserts malware into organizational information systems and information system components (e.g., commercial information technology products), specifically targeted to the hardware, software, and firmware used by organizations (based on knowledge gained via reconnaissance).
	Insert specialized malware into organizational information systems based on system configurations.	Adversary inserts specialized, non-detectable, malware into organizational information systems based on system configurations, specifically targeting critical information system components based on reconnaissance and placement within organizational information systems.
	Insert counterfeit or tampered hardware into the supply chain.	Adversary intercepts hardware from legitimate suppliers. Adversary modifies the hardware or replaces it with faulty or otherwise modified hardware.
	Insert tampered critical components into organizational systems.	Adversary replaces, through supply chain, subverted insider, or some combination thereof, critical information system components with modified or corrupted components.
	Install general-purpose sniffers on organization-controlled systems or networks.	Adversary installs sniffing software onto internal organizational information systems or networks.
	Install persistent and targeted sniffers on organizational information systems and networks.	Adversary places within internal organizational systems or networks software designed to (over a continuous period) collect (sniff) network traffic.
	Insert subverted individuals into organizations.	Adversary places individuals within organizations who are willing and able to conduct actions to cause harm to organizational missions/business functions.

Threat Events	Tactics, Techniques, and Procedures	Description
	Insert subverted individuals into privileged positions in organizations.	Adversary places individuals in privileged positions within organizations who are willing and able to conduct actions to cause harm to organizational missions/business functions. Adversary may target privileged functions to gain access to sensitive information (e.g., user accounts, system files) and may leverage access to one privileged capability to get to another capability.
	Insert untargeted malware into downloadable software and/or into commercial information technology products.	Adversary corrupts or inserts malware into common freeware, shareware, or commercial information technology products. Adversary is not targeting specific organizations, simply looking for entry points into internal organizational information systems. Note that this is particularly a concern for mobile applications.
	Deliver modified malware to internal organizational information systems.	Adversary uses common delivery mechanisms to install/insert known malware (e.g., malware whose existence is known) into organizational information systems.
Exploit and Compromise	Exploit poorly configured or unauthorized systems exposed to the Internet.	Adversary gains access through the Internet to systems that are not authorized for Internet connectivity or that do not meet organizational configuration requirements.
	Exploit recently discovered vulnerabilities.	Adversary exploits recently discovered vulnerabilities in DMS internal information systems in an attempt to compromise the systems before mitigation measures are available or in place.
	Exploit vulnerabilities on DMS internal information systems.	Adversary searches for known vulnerabilities in DMS internal information systems and exploits those vulnerabilities.
	Exploit vulnerabilities using zero-day attacks.	Adversary employs attacks that exploit as yet unpublicized vulnerabilities. Zero-day attacks are based on adversary insight into the information systems and applications used by organizations as well as adversary reconnaissance of organizations.

Threat Events	Tactics, Techniques, and Procedures	Description
	Compromise design, manufacture, and/or distribution of DMS information system components (including hardware, software, and firmware).	Adversary compromises the design, manufacture, and/or distribution of critical information system components at selected suppliers.
	Compromise critical systems via physical access.	Adversary obtains physical access to organizational information systems and makes modifications.
	Compromise information systems or devices used externally and reintroduced into the enterprise.	Adversary installs malware on information systems or devices while the systems/devices are external to organizations for purposes of subsequently infecting organizations when reconnected.
	Compromise DMS information systems to facilitate exfiltration of data/information.	Adversary implants malware into internal DMS information systems, where the malware over time can identify and then exfiltrate valuable information.
	Compromise software of organizational critical information systems.	Adversary inserts malware or otherwise corrupts critical internal organizational information systems.
	Compromise information systems or devices used externally and reintroduced into the enterprise.	Adversary installs malware on information systems or devices while the systems/devices are external to organizations for purposes of subsequently infecting organizations when reconnected.
	Compromise mission-critical information.	Adversary compromises the integrity of mission-critical information, thus preventing or impeding ability of organizations to which information is supplied, from carrying out operations.
Conduct an Attack (i.e., direct/coordinate attack tools or	Conduct brute force login attempts/password guessing attacks.	Adversary attempts to gain access to organizational information systems by random or systematic guessing of passwords, possibly supported by password cracking utilities.

Threat Events	Tactics, Techniques, and Procedures	Description
activities)	Conduct communications interception attacks.	Adversary takes advantage of communications that are either unencrypted or use weak encryption (e.g., encryption containing publicly known flaws), targets those communications, and gains access to transmitted information and channels.
	Conduct wireless jamming attacks.	Adversary takes measures to interfere with wireless communications so as to impede or prevent communications from reaching intended recipients.
	Conduct attacks using unauthorized ports, protocols and services.	Adversary conducts attacks using ports, protocols, and services for ingress and egress that are not authorized for use by organizations.
	Conduct physical attacks on organizational facilities.	Adversary conducts a physical attack on organizational facilities (e.g., sets a fire).
	Conduct distributed denial-of-service attacks.	Adversary uses multiple compromised information systems to attack a single target, thereby causing denial of service for users of the targeted information systems.
	Conduct targeted DoS attacks.	Adversary targets DoS attacks to critical information systems, components, or supporting infrastructures, based on adversary knowledge of dependencies.
	Conduct externally based session hijacking.	Adversary takes control of (hijacks) already established, legitimate information system sessions between organizations and external entities (e.g., users connecting from off-site locations).
	Conduct externally based network traffic modification (man in the middle) attacks.	Adversary, operating outside organizational systems, intercepts/eavesdrops on sessions between organizational and external systems. Adversary then relays messages between organizational and external systems, making them believe that they are talking directly to each other over a private connection, when in fact the entire communication is controlled by the adversary. Such attacks are of particular concern for organizational use of community, hybrid, and public clouds

Threat Events	Tactics, Techniques, and Procedures	Description
	Conduct internally-based network traffic modification (man in the middle) attacks.	Adversary operating within the organizational infrastructure intercepts and corrupts data sessions.
	Conduct supply chain attacks targeting and exploiting critical hardware, software, or firmware.	Adversary targets and compromises the operation of software (e.g., through malware injections), firmware, and hardware that performs critical functions for organizations. This is largely accomplished as supply chain attacks on both commercial off-the-shelf and custom information systems and components.
<i>Achieve Results (i.e., cause adverse impacts, obtain information)</i>	Obtain sensitive information through network sniffing of external networks.	Adversary with access to exposed wired or wireless data channels that organizations (or organizational personnel) use to transmit information (e.g., kiosks, public wireless networks) intercepts communications.
	Cause integrity loss by polluting or corrupting critical data.	Adversary implants corrupted and incorrect data in critical data, resulting in suboptimal actions or loss of confidence in organizational data/services.
	Obtain unauthorized access.	Adversary with authorized access to organizational information systems, gains access to resources that exceeds authorization.
	Cause deterioration/destruction of critical information system components and functions.	Adversary destroys or causes deterioration of critical information system components to impede or eliminate organizational ability to carry out missions or business functions. Detection of this action is not a concern.
<i>Maintain a Presence or Set of Capabilities</i>	Obfuscate adversary actions.	Adversary takes actions to inhibit the effectiveness of the intrusion detection systems or auditing capabilities within organizations.
<i>Coordinate a Campaign</i>	Coordinate cyberattacks using external (outsider), internal (insider), and supply chain (supplier) attack vectors.	Adversary employs continuous, coordinated attacks, potentially using all three attack vectors for the purpose of impeding organizational operations.

Table 3 provides a high-level characterization of non-adversarial threat events as adapted from NIST SP 800-30.⁽³⁵⁾ A non-adversarial threat event is a threat associated with accident or human error, structural failure, or environmental causes. For non-adversarial threat events, the anticipated severity, duration of the event (as included in the description of the event), and range of effects is considered in determining if relevant controls are selected.

Table 4. Non-Adversarial Threat Events

Threat Event	Description
Incorrect privilege settings.	Authorized privileged user or administrator erroneously assigns a user exceptional privileges or sets privilege requirements on a resource too low.
Spill sensitive information.	Authorized user erroneously contaminates a device, information system, or network by placing on it or sending to it information of a classification/sensitivity which it has not been authorized to handle. The information is exposed to access by unauthorized individuals, and as a result, the device, system, or network is unavailable while the spill is investigated and mitigated.
Communications contention.	Degraded communications performance due to contention.
Unreadable display.	Display unreadable due to aging equipment.
Earthquake at primary location.	Earthquake of organization-defined magnitude at primary location makes location inoperable.
Fire at primary location.	Fire (not due to adversarial activity) at primary location makes location inoperable.
Fire at backup location.	Fire (not due to adversarial activity) at backup location makes location inoperable or destroys backups of software, configurations, data, and/or logs.
Flood at primary location.	Flood (not due to adversarial activity) at primary location makes location inoperable.
Flood at backup location.	Flood (not due to adversarial activity) at backup location makes location inoperable or destroys backups of software, configurations, data, and/or logs.
Hurricane at primary location.	Hurricane of organization-defined strength at primary location makes location inoperable.
Hurricane at backup location.	Hurricane of organization-defined strength at backup location makes location inoperable or destroys backups of software, configurations, data, and/or logs.
Resource depletion.	Degraded processing performance due to resource depletion.
Introduction of vulnerabilities into software products.	Due to inherent weaknesses in programming languages and software development environments, errors and vulnerabilities are introduced into commonly used software products.
Disk error.	Corrupted storage due to a disk error.
Pervasive disk error.	Multiple disk errors due to aging of a set of devices all acquired at the same time, from the same supplier.
Windstorm/tornado at primary location.	Windstorm/tornado of organization-defined strength at primary location makes location inoperable.

Threat Event	Description
Windstorm/tornado at backup location.	Windstorm/tornado of organization-defined strength at backup location makes location inoperable or destroys backups of software, configurations, data, and/or logs.

Table 4 provides an overview of potential threat events that are specific to and even more relevant to the DMS than the general threats listed in table 2 and table 3. These physical object threat events are adapted from NIST SP 800-82,⁽³⁾ which addresses ICS, as ICS are similar in nature and operations to ITS physical objects.

Table 5. Physical Object Threat Events

Threat Event	Description
Denial of control.	Temporarily prevents operators and engineers from interfacing with process controls. An affected process may still be operating during the period of control loss, but not necessarily in a desired state.
Spoofed reporting message.	False information sent to an ITS system operator either for evasion or to impair process control. The adversary could make the defenders and operators think that other errors are occurring in order to distract them from the actual source of the problem (i.e., alarm floods).
Theft of operational information.	Adversaries may steal operational information for personal gain or to inform future operations.
Loss of availability.	Adversaries may leverage malware to delete or encrypt critical data on human-machine interfaces, workstations, or databases.
Loss of safety.	Adversaries may target and disable safety system functions as a prerequisite to subsequent attack execution or to allow for future unsafe conditionals to go unchecked.

Table 5 includes or adapts vulnerabilities and predisposing conditions from NIST SP 800-82.⁽³⁾ A vulnerability is a weakness in a system, system security procedures, internal controls, or implementation that could be exploited by a threat source. Most vulnerabilities can be associated with system- or organization-level controls that either have not been applied (either intentionally or unintentionally) or have been applied but retain some weakness.

A predisposing condition is a condition that exists within an organization, a mission/business process, enterprise architecture, or system including its environment of operation, which contributes to (i.e., increases or decreases) the likelihood that one or more threat events, once initiated, will result in undesirable consequences or adverse impact. Predisposing conditions include, for example, the location of a location in a hurricane- or flood-prone region (increasing the likelihood of exposure to hurricanes or floods) or a stand-alone system with no external network connectivity (decreasing the likelihood of exposure to a network-based attack).

Vulnerabilities resulting from predisposing conditions that cannot be easily corrected could include, for example, gaps in contingency plans, use of outdated technologies, or weaknesses/deficiencies in system backup and failover mechanisms.

The groups of vulnerabilities are:

- Policy and Procedures
- System
 - Architecture and Design
 - Configuration and Maintenance
 - Physical
 - Software Development
 - Communication and Network Configuration

Table 6. Vulnerabilities and Predisposing Conditions

Vulnerability		Description
<i>Policy and Procedure Vulnerabilities and Predisposing Conditions</i>	Inadequate security policy for ITS.	Vulnerabilities are often introduced into the ITS environment due to inadequate policies or the lack of policies specifically for ITS security. Controls and countermeasures should be derived from a risk assessment or policy. This ensures uniformity and accountability.
	Malware protection implemented without sufficient testing.	Malware protection software deployed without sufficient testing could impact normal operation of the ITS and block the system from performing necessary control actions.
	Inadequate organizational ownership of risk assessments.	Risk assessments should be performed with acknowledgement from appropriate levels within the organization. Lack of understanding of risk could lead to under-mitigated scenarios or inadequate funding and selection of controls.
	Inadequate security policy for ITS.	Vulnerabilities are often introduced into the ITS environment due to inadequate policies or the lack of policies specifically for ITS security. Controls and countermeasures should be derived from a risk assessment or policy. This ensures uniformity and accountability.
	Inadequate ITS security training and awareness program.	A documented formal ITS security training and awareness program is designed to keep staff up to date on organizational security policies and procedures, threats, industry cybersecurity standards, and recommended practices. Without adequate ongoing training on specific ITS policies and procedures, staff cannot be expected to maintain a secure ITS environment.

Vulnerability		Description
	Lack of inventory management policy.	Inventory policy and procedures should include installation, removal, and changes made to hardware, firmware, and software. An incomplete inventory could lead to unmanaged and unprotected devices within the ITS environment.
	Lack of configuration management policy.	Lack of policy and procedures for ITS configuration management can lead to an unmanageable and highly vulnerable inventory of hardware, firmware, and software.
	Lack of redundancy for critical components.	Lack of redundancy in critical components could provide single-point-of failure possibilities
	Inadequate incident detection & response plan and procedures.	Incident detection and response plans, procedures, and methods are necessary for rapidly detecting incidents, minimizing loss and destruction, preserving evidence for later forensic examination, mitigating the weaknesses that were exploited, and restoring services. Establishing a successful incident response capability includes continually monitoring for anomalies, prioritizing the handling of incidents, and implementing effective methods of collecting, analyzing, and reporting data.
	Malware protection implemented without sufficient testing.	Malware protection software that is deployed without sufficient testing could impact normal operation of the OT and block the system from performing necessary control actions.
	Intrusion detection and prevention software is not installed.	Incidents can result in loss of system availability and integrity; the capture, modification, and deletion of data; and incorrect execution of control commands. Intrusion detection system/intrusion protection system (IDS/IPS) software may stop or prevent various types of attacks, including DoS attacks, and also identify attacked internal hosts, such as those infected with worms. IDS/IPS software must be tested prior to deployment to ensure that it does not compromise normal operation of the OT.
Architecture and Design Vulnerabilities and Predisposing Conditions	No security perimeter defined.	If the OT does not have a security perimeter clearly defined, it is not possible to ensure that the necessary security controls are deployed and configured properly. This can lead to unauthorized access to systems and data, as well as other problems
	Control networks used for non-control traffic.	Control and non-control traffic have different requirements, such as determinism and reliability, so having both types of traffic on a single network

Vulnerability		Description
		makes it more difficult to correctly configure the network so that it meets the requirements of the control traffic, and that complexity can create undue risk. For example, non-control traffic could inadvertently consume resources that control traffic needs, causing disruptions in physical object functions. There may also be the potential for lateral movement from the non-control traffic to the control traffic, which could lead to hijacking or other types of attacks.
	Inadequate incorporation of security into architecture and design.	Incorporating security into the physical object architecture, design must start with budget, and schedule of the physical object. The security architecture is part of the Enterprise Architecture. The architectures must address the identification and authorization of users, access control mechanism, network topologies, and system configuration and integrity mechanisms.
	Inadequate collection of event data history.	Forensic analysis depends on collection and retention of enough data. Without proper and accurate data collection, it might be impossible to determine what caused a security incident to occur. Incidents might go unnoticed, leading to additional damage and/or disruption. Regular monitoring is also needed to identify problems with controls, such as misconfigurations and failures.
Configuration and Maintenance Vulnerabilities and Predisposing Conditions	Hardware, firmware, and software not under asset management.	The organization doesn't know what it has (e.g., make, model), where they are, or what version it has, resulting in an inconsistent and ineffective defense posture. To properly secure an ITS, there should be an accurate inventory of the assets in the environment. Procedures should be in place to manage additions, deletions, and modifications of assets which include asset inventory management. These procedures are critical to executing business continuity and disaster recovery plans.
	Hardware, firmware, and software are not under configuration management.	The organization doesn't know the DMS management status, security settings, or configuration versions that it has, resulting in inconsistent and ineffective defense posture. A lack of configuration change management procedures can lead to security oversights, exposures, and risks. A process for controlling modifications to hardware, firmware, software, and documentation should be implemented to ensure an ITS is protected against inadequate or improper modifications before, during, and after system implementation. To properly secure

Vulnerability	Description
	an ITS, there should be an accurate listing or repository of the current configurations.
	Lack of a vulnerability management program. Vulnerabilities not considered by the organization could result in exploitation. Vulnerability management procedures should be in place to determine a plan of action or inaction upon discovery of a vulnerability. Some ITS considerations are availability concerns may push patching until the next planned operational downtime; security patch support may not be available for ITS systems that use outdated operating systems; isolated systems may not require immediate patching; and ITS exposed to the internet may need prioritized for patching.
	Operating system and vendor software DMS may not be developed until long after security vulnerabilities are found. Out-of-date operating systems and applications may contain newly discovered vulnerabilities that could be exploited. Security DMS support may not be available for legacy OT, so vulnerability management procedures should include contingency plans for mitigating vulnerabilities where DMS may never be available or replacement plans
	Inadequate testing of security changes. Modifications to hardware, firmware, and software deployed without testing could compromise normal operation of the ITS. Documented procedures should be developed for testing all changes for security impact. The live operational systems should never be used for testing. The testing of system modifications may need to be coordinated with system vendors and integrators.
	Poor remote access controls. There are many reasons why an OT may need to be remotely accessed, including vendors and system integrators performing system maintenance functions or OT engineers accessing geographically remote system components. The concept of least privilege should be applied to remote access controls. Remote access capabilities must be adequately controlled to prevent unauthorized individuals from gaining access or authorized individuals from gaining excessive access to the OT.
	Poor configurations are used. Improperly configured systems may leave unnecessary ports and protocols open. These unnecessary functions may contain vulnerabilities that increase the overall risk to the system. Using default configurations often exposes vulnerabilities and exploitable services. All settings should be examined.

Vulnerability		Description
	Critical configurations are not stored or backed up.	Procedures should be available for restoring ITS configuration settings in the event of accidental or adversary-initiated configuration changes to maintain system availability and prevent loss of data. Documented procedures should be developed for maintaining configuration settings.
	Inadequate access controls applied.	Access controls must be DMS to the way the organization allocates responsibilities and privilege to its personnel. Poorly specified access controls can result in giving an ITS user too many or too few privileges. The following exemplify each case: • System configured with default access control settings gives an operator administrative privileges • System configured improperly results in an operator being unable to take corrective actions in an emergency
	Malware protection is not installed or up to date.	For physical objects that include an operating system and possibly applications, installation of malicious software, or malware, is a common attack. Malware protection software, such as antivirus software, should be kept current in a very dynamic environment. Outdated malware protection software and definitions leave the system open to malware threats
	DoS.	Physical object software could be vulnerable to DoS attacks, resulting in the prevention of authorized access to a system resource or delaying system operations and functions.
	Passwords generation, use, and protection not in accord with policy.	Password policy and procedure must be followed to be effective. Violations of password policy and procedures can increase physical object vulnerability.
	Logs are not maintained.	Without proper and accurate logs, it might be impossible to determine what caused a security event to occur and perform adequate forensics.
Physical Vulnerabilities and Predisposing Conditions	Unauthorized personnel have physical access to equipment.	Physical access to physical object equipment should be restricted to only the necessary personnel, considering safety requirements, such as emergency shutdown or restarts. Unauthorized access to physical object equipment can lead to any of the following: • Physical theft of data and hardware

Vulnerability		Description
		- Physical damage or destruction of data and hardware - Modification of the operational process - Unauthorized changes to or uses of the functional environment (e.g., data connections use of removable media, adding/removing resources) - Disconnection of physical data links - Undetectable interception of data (keystroke and other input logging)
	Radio frequency, EMP, static discharge, brownouts, and voltage spikes.	Some hardware used for OT systems is vulnerable to radio frequency, EMPs, static discharge, brownouts, and voltage spikes. The impacts can range from the temporary disruption of command and control to permanent damage to circuit boards. Proper shielding, grounding, power conditioning, and/or surge suppression is recommended
	Lack of backup power.	Without backup power to critical assets, a general loss of power will shut down the OT and could create an unsafe situation. Loss of power could also lead to insecure default settings. If the program file or data is stored in volatile memory, the process may not be able to restart after a power outage without appropriate backup power.
	Loss of environmental control.	The loss of environmental control (e.g., temperatures, humidity) could lead to equipment damage, such as processors overheating. Some processors will shut down to protect themselves. Others may continue to operate in a minimal capacity and produce intermittent errors, continually reboot, or become permanently inoperable.
Software Development Vulnerabilities and Predisposing Conditions	Inadequate authentication, privileges, and access control in software.	Unauthorized access to configuration and programming software could provide the ability to corrupt a device.
	Data flow controls are not employed.	Data flow controls based on data characteristics are needed to restrict the information that is permitted between systems. These controls can prevent the exfiltration of information and illegal operations
Communication and Network Configuration Vulnerabilities and	Firewalls are nonexistent or improperly configured.	A lack of properly configured firewalls could permit unnecessary data to pass between networks, such as control and corporate networks, thus allowing attacks and malware to spread between networks, making sensitive

Vulnerability		Description
Predisposing Conditions	Standard, well-documented communication protocols are used in plaintext.	Adversaries that can monitor the OT network activity can use a protocol analyzer or other utilities to decode the data transferred by protocols, such as telnet, FTP, Hypertext Transfer Protocol, and Network File System. The use of such protocols also makes it easier for adversaries to perform attacks against the OT and manipulate OT network activity.
	Use of unsecure OT protocols.	OT protocols often have few or no security capabilities, such as authentication and encryption, to protect data from unauthorized access or tampering. The incorrect implementation of the protocols can also lead to additional vulnerabilities.
	Lack of integrity checking for communications.	Integrity checks are not built into most OT protocols, so adversaries could manipulate communications undetected. To ensure integrity, the OT can use lower-layer protocols (e.g., IPSec) that offer data integrity protection when traversing untrusted physical media.
	Inadequate authentication between wireless clients and access points.	Strong mutual authentication between wireless clients and access points is needed to ensure that legitimate OT clients do not connect to a rogue access point deployed by an adversary and that adversary clients do not connect to any of the OT wireless networks
	Inadequate data protection between wireless clients and access points.	Sensitive data between wireless clients and access points should be protected using strong encryption to ensure that adversaries cannot gain unauthorized access to the unencrypted data.
	Inadequate incorporation of security into architecture and design.	Incorporating security into the ITS architecture and design must start with a budget and schedule designated for ITS. The architectures must address the identification and authorization of users, access control mechanism, network topologies, and system configuration and integrity mechanisms.
	Inappropriate segmentation of the asset management system.	Most architectures are designed for PLCs, remote terminal units, distributed control systems, and SCADA controllers to manipulate the process and for asset management systems to monitor the assets connected to the controllers. Many asset management systems also have the technical ability to modify the configuration of sensors and final elements, although modification may not be their primary function. The asset management system should be controlled appropriately based on its ability (or lack of ability) to manipulate the process.

Vulnerability		Description
	Intrusion detection/prevention software not installed.	Incidents can result in loss of system availability and integrity; the capture, modification, and deletion of data; and incorrect execution of control commands. IDS/IPS software may stop or prevent various types of attacks, including DoS attacks, and identify attacked internal hosts, such as those infected with worms. IDS/IPS software must be tested prior to deployment to determine that it does not compromise normal operation of the physical object.
	Authentication of users, data or devices is substandard or nonexistent.	Without authentication, there is the potential to replay, modify, or spoof data; or to spoof device identities or user identities; or masquerade devices.
Sensor, Final Element, and Asset Management Vulnerabilities and Predisposing Conditions	Unauthorized physical access to sensors or final elements.	Physical access to sensors and final elements allows for direct manipulation of the physical process. Many smart devices are configured on a fieldbus such that electronic access to the sensor network allows for manipulation of controlling parameters. Physical access to the whole of the loop should be managed to prevent incidents.
	Unauthorized wireless access to sensors or final elements.	Wireless access to sensors and final elements allows for direct manipulation of the physical process. Many smart devices allow for wireless configuration. Wireless access should be securely configured or disabled using hardware write-protect where possible to protect unauthorized modification of the sensors and final elements which are connected both to the physical process and to the physical object environment.
	Inappropriate segmentation of asset management system.	Most architectures are designed for PLCs, remote terminal unit, distributed control system, and SCADA controllers to manipulate the process, and for asset management systems to monitor the assets connected to the controllers. Many asset management systems also have the technical ability to modify the configuration of sensors and final elements, although modification may not be their primary function. The asset management system should be controlled appropriately based on its ability (or lack of ability) to manipulate the process.

Appendix B. NIST SP 800-53 Security Control's Mapping

Table 7. Mapping of DMS Mission Objectives to NIST CSF Subcategories and NIST SP 800-53 Controls

Objectives	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
Mission Objective #1: Improve Physical Safety of the Transportation Ecosystem	GV.OC-01: The organizational mission is understood and informs cybersecurity risk management.	3	PM-11: Mission and Business Process Definition	PM-11 was not chosen because mission and business process definitions are organizational, with DMS focusing on tactical message display functions.
	GV.OC-02: Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered.	2	PM-09: Risk Management Strategy PM-30: Supply Chain Risk Management Strategy SR-03: Supply Chain Controls and Processes SR-06: Supplier Assessments and Reviews	
	GV.OC-03: Legal, regulatory, and contractual requirements regarding cybersecurity — including privacy and civil liberties obligations — are understood and managed.	3	MA-01: Policy and Procedures MP-01: Policy and Procedures PE-01: Policy and Procedures PL-01: Policy and Procedures PM-01: Information Security Program Plan PS-01: Policy and Procedures PT-01: Policy and Procedures	MA-1 was not chosen because maintenance policies are low priority for DMS, which undergo periodic hardware checks rather than requiring extensive procedural frameworks. MP-1 was not chosen because media protection policies are minimally relevant to DMS,

U.S. Department of Transportation
Office of the Assistant Secretary for Research and Technology
Intelligent Transportation Systems Joint Program Office

Objectives	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
			RA-01: Policy and Procedures SA-01: Policy and Procedures SC-01: Policy and Procedures SI-01: Policy and Procedures SR-01: Policy and Procedures PM-28: Risk Framing	which lack significant removable media or data storage components. PE-1 was not chosen because physical and environmental protection policies are moderate priority but not selected due to DMS's inherent robustness in outdoor deployments. PL-1 was not chosen because planning policies are organizational-level and less critical for the operational focus of DMS field devices. PM-1 was not chosen because information security program policies are broad and handled at the enterprise level, not specifically for DMS systems. PS-1 was not chosen because personnel security policies are low priority due to limited human interaction with DMS systems. PT-1 was not chosen because personally identifiable information processing and transparency policies are not applicable, as DMS do not

Objectives	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
				handle personally identifiable information. SA-1 was not chosen because system and services acquisition policies are organizational and not device-specific for DMS procurement. SC-1 was not chosen because system and communications protection policies are covered by higher-priority technical controls for DMS. SI-1 was not chosen because system integrity policies are low priority, with integrity ensured through other operational controls for DMS. SR-1 was not chosen because supply chain risk management policies are low priority for DMS with fewer dependencies. PM-28 was not chosen because risk framing is an enterprise-level activity, not specific to DMS field devices. RA-1 was not chosen because risk assessment policies are lower priority for DMS, focusing

Objectives	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
				on communication risks rather than broad assessments.
	GV.OC-04: Critical objectives, capabilities, and services that external stakeholders depend on or expect from the organization are understood and communicated.	3	PM-08: Critical Infrastructure Plan PM-11: Mission and Business Process Definition CP-02(08): Identify Critical Assets PM-30(01): Suppliers of Critical or Mission-Essential Items RA-09: Criticality Analysis	PM-8 was not chosen because critical infrastructure planning is addressed at the broader ITS network level, not for stand-alone DMS. CP-2(08) was not chosen because developing detailed contingency plans is less applicable to DMS, which have simpler operational roles and rely on network-level redundancies rather than device-specific planning. RA-09 was not chosen because criticality analysis for mission-essential functions is conducted at the ITS portfolio level, not for specific DMS instances, to prioritize resources across transportation assets.
	GV.OC-05: Outcomes, capabilities, and services that the organization depends on are understood and communicated.	3	PM-11: Mission and Business Process Definition PM-30: Supply Chain Risk Management Strategy RA-07: Risk Response SA-09: External System Services	SR-5 was not chosen because acquisition strategies for supply chain risk are organizational, not specific to DMS deployment.

Objectives	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
			SR-05: Acquisition Strategies, Tools, and Methods	
	GV.RM-01: Risk management objectives are established and agreed to by organizational stakeholders.	3	PM-09: Risk Management Strategy RA-07: Risk Response SR-02: Supply Chain Risk Management Plan	
	GV.RM-05: Lines of communication across the organization are established for cybersecurity risks, including risks from suppliers and other third parties.	3	PM-09: Risk Management Strategy PM-30: Supply Chain Risk Management Strategy	
	GV.RM-06: A standardized method for calculating, documenting, categorizing, and prioritizing cybersecurity risks is established and communicated.	3	PM-09: Risk Management Strategy PM-18: Privacy Program Plan PM-28: Risk Framing PM-30: Supply Chain Risk Management Strategy RA-03: Risk Assessment	PM-18 was not chosen because privacy program planning is irrelevant for DMS, which do not process personally identifiable information.
	GV.RM-07: Strategic opportunities (i.e., positive risks) are characterized and are included in organizational	3	PM-09: Risk Management Strategy PM-18: Privacy Program Plan PM-28: Risk Framing PM-30: Supply Chain Risk Management Strategy	

Objectives	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
	cybersecurity risk discussions.		RA-03: Risk Assessment	
	GV.RR-03: Adequate resources are allocated commensurate with the cybersecurity risk strategy, roles, responsibilities, and policies.	3	PM-02: Information Security Program Leadership Role PM-19: Privacy Program Leadership Role PM-23: Data Governance Body PM-24: Data Integrity Board PM-29: Risk Management Program Leadership Roles	PM-2 was not chosen because defining leadership roles for information security is an organizational function, not device-specific for DMS. PM-19 was not chosen because privacy leadership roles are organizational and not applicable to DMS systems handling non-sensitive data. PM-23 was not chosen because data governance is a low priority for DMS, which manages limited traffic-related data without complex oversight needs. PM-24 was not chosen because data integrity oversight is covered by technical controls, not requiring a dedicated board for DMS operations. PM-29 was not chosen because risk management leadership is organizational, with DMS risks integrated into broader ITS strategies.
	GV.OV-01: Cybersecurity risk management strategy	3	PM-11: Mission and Business Process Definition	

Objectives	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
	outcomes are reviewed to inform and adjust strategy and direction.		PM-30: Supply Chain Risk Management Strategy RA-07: Risk Response SA-09: External System Services SR-05: Acquisition Strategies, Tools, and Methods	
	GV.SC-01: A cybersecurity supply chain risk management program, strategy, objectives, policies, and processes are established and agreed to by organizational stakeholders.	3	PM-30: Supply Chain Risk Management Strategy SR-02: Supply Chain Risk Management Plan SR-03: Supply Chain Controls and Processes	
	GV.SC-03: Cybersecurity supply chain risk management is integrated into cybersecurity and enterprise risk management, risk assessment, and improvement processes.	3	AC-01: Policy and Procedures AT-01: Policy and Procedures AU-01: Policy and Procedures CA-01: Policy and Procedures CM-01: Policy and Procedures CP-01: Policy and Procedures IA-01: Policy and Procedures IR-01: Policy and Procedures MA-01: Policy and Procedures MP-01: Policy and Procedures PE-01: Policy and Procedures PL-01: Policy and Procedures	AT-1 was not chosen because it focuses on developing organizational-level security awareness and training policies, which are less critical for DMS systems that operate with minimal human interaction and limited user training needs. CA-1 was not chosen because it pertains to organizational policies for security assessments and authorizations, which are managed at a broader ITS level rather than specifically for field

Objectives	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
			PM-01: Information Security Program Plan PS-01: Policy and Procedures PT-01: Policy and Procedures RA-01: Policy and Procedures SA-01: Policy and Procedures SC-01: Policy and Procedures SI-01: Policy and Procedures SR-01: Policy and Procedures PM-09: Risk Management Strategy PM-18: Privacy Program Plan PM-30: Supply Chain Risk Management Strategy PM-31: Continuous Monitoring Strategy SR-02: Supply Chain Risk Management Plan SR-03: Supply Chain Controls and Processes RA-03: Risk Assessment RA-07: Risk Response	devices like DMS with focused operational risks. CM-01 This control establishes overarching organizational policies and procedures for configuration management, which is addressed at the ITS enterprise level rather than the field-specific DMS device to avoid redundancy in device-level implementations. CP-1 was not chosen because contingency planning policies are lower priority for DMS, as these devices are not central to complex recovery processes and are covered by higher-level ITS recovery strategies. IA-1 was not chosen because identification and authentication policies are low priority for DMS, which often use preconfigured access rather than dynamic user management. PM-31 was not because continuous monitoring strategies are moderate priority but handled at the network level rather than DMS-specific.

Objectives	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
	GV.SC-04: Suppliers are known and prioritized by criticality.	3	RA-09: Criticality Analysis SA-09: External System Services SR-06: Supplier Assessments and Reviews	SC-04 was not chosen because DMS does not share resources with other systems in a multi-tenant environment, as it operates as a dedicated field endpoint with isolated communications to the TMS.
	GV.SC-05: Requirements to address cybersecurity risks in supply chains are established, prioritized, and integrated into contracts and other types of agreements with suppliers and other relevant third parties.	3	SA-04: Acquisition Process SA-09: External System Services SR-03: Supply Chain Controls and Processes SR-05: Acquisition Strategies, Tools, and Methods SR-06: Supplier Assessments and Reviews SR-10: Inspection of Systems or Components	
	GV.SC-06: Planning and due diligence are performed to reduce risks before entering into formal supplier or other third-party relationships.	3	SA-04: Acquisition Process SA-09: External System Services SR-05: Acquisition Strategies, Tools, and Methods SR-06: Supplier Assessments and Reviews	
	GV.SC-07: The risks posed by a supplier, their products and services, and other third parties are understood, recorded,	3	RA-09: Criticality Analysis SA-04: Acquisition Process SA-09: External System Services	

Objectives	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
	prioritized, assessed, responded to, and monitored over the course of the relationship.		SR-03: Supply Chain Controls and Processes SR-06: Supplier Assessments and Reviews	
	GV.SC-09: Supply chain security practices are integrated into cybersecurity and enterprise risk management programs, and their performance is monitored throughout the technology product and service lifecycle.	3	PM-09: Risk Management Strategy PM-19: Privacy Program Leadership Role PM-28: Risk Framing PM-30: Supply Chain Risk Management Strategy PM-31: Continuous Monitoring Strategy RA-03: Risk Assessment RA-07: Risk Response SA-04: Acquisition Process SA-09: External System Services SR-02: Supply Chain Risk Management Plan SR-03: Supply Chain Controls and Processes SR-05: Acquisition Strategies, Tools, and Methods SR-06: Supplier Assessments and Reviews	
	GV.SC-10: Cybersecurity supply chain risk management plans include	3	PM-31: Continuous Monitoring Strategy	

Objectives	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
	provisions for activities that occur after the conclusion of a partnership or service agreement.		RA-03: Risk Assessment RA-05: Vulnerability Monitoring and Scanning RA-07: Risk Response SA-04: Acquisition Process SA-09: External System Services SR-02: Supply Chain Risk Management Plan SR-03: Supply Chain Controls and Processes SR-05: Acquisition Strategies, Tools, and Methods SR-06: Supplier Assessments and Reviews	
	ID.AM-01: Inventories of hardware managed by the organization are maintained.	3	CM-08: System Component Inventory PM-05: System Inventory	
	ID.AM-02: Inventories of software, services, and systems managed by the organization are maintained.	3	AC-20: Use of External Systems CM-08: System Component Inventory PM-05: System Inventory SA-05: System Documentation SA-09: External System Services	
	ID.AM-08: Systems, hardware, software, services, and data are	3	CM-09: Configuration Management Plan CM-13: Data Action Mapping	PM-22 was not chosen because DMS does not handle personally identifiable information, making

Objectives	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
	managed throughout their lifecycles.		MA-02: Controlled Maintenance MA-06: Timely Maintenance PL-02: System Security and Privacy Plans PM-22: Personally Identifiable Information Quality Management PM-23: Data Governance Body SA-03: System Development Lifecycle SA-04: Acquisition Process SA-08: Security and Privacy Engineering Principles SA-22: Unsupported System Components SI-12: Information Management and Retention SI-18: Personally Identifiable Information Quality Operations SR-05: Acquisition Strategies, Tools, and Methods SR-12: Component Disposal	quality management controls unnecessary. SA-03 was not chosen because integrating security into the system development lifecycle is moderate priority but managed during ITS system design, not DMS alone. SI-18 was not chosen because personally identifiable information quality operations are irrelevant for DMS systems that do not process or store personally identifiable information. CM-13 was not chosen because the DMS primarily handles predefined, real-time message updates and status reporting without complex user-driven data actions, rendering this control's requirement for mapping data flows to specific actions overly granular and not applicable. SI-12 was not chosen because log based controls within this document covers the management and retention of information.

Objectives	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
	ID.RA-04: Potential impacts and likelihoods of threats exploiting vulnerabilities are identified and recorded.	3	PM-09: Risk Management Strategy PM-11: Mission and Business Process Definition RA-02: Security Categorization RA-03: Risk Assessment RA-08: Privacy Impact Assessments RA-09: Criticality Analysis	RA-02 was not chosen because security categorization of the overall ITS system, including DMS, is performed at the program level rather than per device to align with federal categorization standards. RA-08 was not chosen because privacy assessments focus on personal data handling, which is minimal in DMS operations that display aggregate traffic information without collecting or processing identifiable driver data.
	ID.RA-05: Threats, vulnerabilities, likelihoods, and impacts are used to understand inherent risk and inform risk response prioritization.	3	PM-16: Threat Awareness Program RA-02: Security Categorization RA-03: Risk Assessment RA-07: Risk Response	PM-16 was not chosen because threat awareness programs are organizational and not device-specific for DMS operations.
	ID.RA-06: Risk responses are chosen, prioritized, planned, tracked, and communicated.	3	PM-09: Risk Management Strategy PM-18: Privacy Program Plan PM-30: Supply Chain Risk Management Strategy RA-07: Risk Response	
	ID.RA-08: Processes for receiving, analyzing, and responding to vulnerability	3	RA-05: Vulnerability Monitoring	

Objectives	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
	disclosures are established.			
	ID.RA-10: Critical suppliers are assessed prior to acquisition.	3	SR-06: Supplier Assessments and Reviews	
	ID.IM-01: Improvements are identified from evaluations.	3	AC-01: Policy and Procedures AT-01: Policy and Procedures AU-01: Policy and Procedures CA-01: Policy and Procedures CM-01: Policy and Procedures CP-01: Policy and Procedures IA-01: Policy and Procedures IR-01: Policy and Procedures MA-01: Policy and Procedures MP-01: Policy and Procedures PE-01: Policy and Procedures PL-01: Policy and Procedures PM-01: Information Security Program Plan PS-01: Policy and Procedures PT-01: Policy and Procedures RA-01: Policy and Procedures SA-01: Policy and Procedures SC-01: Policy and Procedures SI-01: Policy and Procedures	CA-2 was not chosen because periodic security assessments are less frequent and critical for standalone DMS devices compared to more interconnected network systems, prioritizing operational integrity over comprehensive evaluations. CP-2 was not chosen because developing detailed contingency plans is less applicable to DMS, which have simpler operational roles and rely on network-level redundancies rather than device-specific planning.

Objectives	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
			SR-01: Policy and Procedures CA-02: Control Assessments CA-05: Plan of Action and Milestones CA-07: Continuous Monitoring CA-08: Penetration Testing CP-02: Contingency Plan IR-04: Incident Handling IR-08: Incident Response Plan PL-02: System Security and Privacy Plans RA-03: Risk Assessment RA-05: Vulnerability Monitoring and Scanning RA-07: Risk Response SA-08: Security and Privacy Engineering Principles SA-11: Developer Testing and Evaluation SA-17(06): Structure For Testing SI-02: Flaw Remediation SI-04: System Monitoring SR-05: Acquisition Strategies, Tools, and Methods	
	ID.IM-02: Improvements are identified from security tests and exercises, including those done in	3	Same controls as ID.IM-01	

Objectives	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
	coordination with suppliers and relevant third parties.			
	ID.IM-03: Improvements are identified from execution of operational processes, procedures, and activities.	3	Same controls as ID-IM-01	
	ID.IM-04: Incident response plans and other cybersecurity plans that affect operations are established, communicated, maintained, and improved.	3	CP-02: Contingency Plan IR-08: Incident Response Plan PL-02: System Security and Privacy Plans SR-02: Supply Chain Risk Management Plan	
	PR.AA-01: Identities and credentials for authorized users, services, and hardware are managed by the organization.	2	AC-02: Account Management IA-03: Device Identification and Authentication IA-06: Authentication Feedback IA-08: Identification and Authentication (Non-Organizational Users) IA-11: Re-authentication	
	PR.AA-06: Physical access to assets is managed, monitored, and enforced commensurate with risk.	2	PE-02: Physical Access Authorizations PE-03: Physical Access Control PE-06: Monitoring Physical Access	

Objectives	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
	PR.AT-01: Personnel are provided with awareness and training so that they possess the knowledge and skills to perform general tasks with cybersecurity risks in mind.	3	AT-02: Literacy Training and Awareness AT-03: Role-Based Training	AT-2 was not chosen because DMS systems have limited direct user interaction, reducing the necessity for extensive literacy training and awareness programs tailored to general personnel.
	PR.PS-03: Hardware is maintained, replaced, and removed commensurate with risk.	3	CM-07(09): Prohibiting The Use of Unauthorized Hardware SA-10(03): Hardware Integrity Verification SC-03(01): Hardware Separation SC-39(01): Hardware Separation SC-49: Hardware-Enforced Separation and Policy Enforcement SC-51: Hardware-Based Protection	SC-49 & SC-51 was not chosen because SC-39(1) sufficiently provides guidance for hardware separation and protection.
	PR.PS-05: Installation and execution of unauthorized software are prevented.	3	CM-07(02): Prevent Program Execution CM-07(04): Unauthorized Software — Deny-By-Exception CM-07(05): Authorized Software — Allow by Exception SC-34: Non-Modifiable Executable Programs	SC-34 was not chosen because DMS firmware is designed to be non-modifiable in the field via physical enclosures and access controls, aligning with this control inherently without additional specifications.
	PR.IR-02: The organization's technology	2	PE-09: Power Equipment and Cabling PE-11: Emergency Power	SC-36 was not chosen because distributed processing and storage are not applicable to

Objectives	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
	assets are protected from environmental threats.		PE-14: Environmental Controls	DMS, which perform localized functions without distributed components.
	PR.IR-03: Mechanisms are implemented to achieve resilience requirements in normal and adverse situations.	3	SA-08: Security and Privacy Engineering Principles SC-06: Resource Availability SC-24: Fail In Known State SC-36: Distributed Processing and Storage SC-39: Process Isolation SI-13: Predictable Failure Prevention	SI-13 was not chosen because SC-24 <i>Fail in Known State</i> provides sufficient guidance for securing failures to the DMS system.
	PR.IR-04: Adequate resource capacity to ensure availability is maintained.	3	CP-06: Alternate Storage Site CP-07: Alternate Processing Site CP-08: Telecommunications Services PM-03: Information Security and Privacy Resources PM-09: Risk Management Strategy	CP-6 was not chosen because DMS systems store minimal data, making alternate storage sites unnecessary for their basic message display functionality. CP-7 was not chosen because DMS are physical field devices with no need for alternate processing sites, as processing is distributed and resilient within the ITS network.
	DE.CM-01: Networks and network services are monitored to find potentially adverse events.	3	AC-02: Account Management AU-12: Audit Record Generation CA-07: Continuous Monitoring CM-03: Configuration Change Control SC-05: Denial-of-Service Protection	PM-3 was not chosen because resource allocation for security and privacy is managed programmatically, not at the DMS device level.

Objectives	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
			SC-07: Boundary Protection SI-04: System Monitoring	
	DE.CM-02: The physical environment is monitored to find potentially adverse events.	2	CA-07: Continuous Monitoring PE-03: Physical Access Control PE-06: Monitoring Physical Access	
	DE.AE-04: The estimated impact and scope of adverse events are understood.	3	PM-09: Risk Management Strategy PM-11: Mission and Business Process Definition PM-18: Privacy Program Plan PM-28: Risk Framing PM-30: Supply Chain Risk Management Strategy	
	RS.MA-01: The incident response plan is executed in coordination with relevant third parties once an incident is declared.	3	IR-06: Incident Reporting IR-08: Incident Response Plan SR-03: Supply Chain Controls and Processes SR-08: Notification Agreements	SR-8 was not chosen because notification agreements for supply chain compromises are handled at the enterprise level, not for individual DMS.
	RS.MA-02: Incident reports are triaged and validated.	3	IR-04: Incident Handling IR-05: Incident Monitoring IR-06: Incident Reporting	
	RS.MA-03: Incidents are categorized and prioritized.	3	IR-04: Incident Handling IR-05: Incident Monitoring IR-06: Incident Reporting	

Objectives	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
	RS.MA-04: Incidents are escalated or elevated as needed.	3	IR-04: Incident Handling IR-05: Incident Monitoring IR-06: Incident Reporting IR-07: Incident Response Assistance	IR-07 was not chosen because this control pertains to providing assistance during incidents across the organization, which is handled by centralized ITS support teams rather than decentralized DMS field equipment.
	RS.MA-05: The criteria for initiating incident recovery are applied.	3	IR-04: Incident Handling IR-08: Incident Response Plan	IR-08 was not chosen because a comprehensive incident response plan is developed and maintained at the ITS system level, not for isolated DMS devices, to ensure coordinated response across the transportation infrastructure.
	RS.MI-01: Incidents are contained.	3	IR-04: Incident Handling	
	RS.CO-02: Internal and external stakeholders are notified of incidents.	3	IR-04: Incident Handling IR-06: Incident Reporting IR-07: Incident Response Assistance SR-03: Supply Chain Controls and Processes SR-08: Notification Agreements	
	RS.MI-01: Incidents are contained.	3	IR-04: Incident Handling	

Objectives	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
	RS.MI-02: Incidents are eradicated.	3	IR-04: Incident Handling	
	RC.RP-01: The recovery portion of the incident response plan is executed once initiated from the incident response process.	3	CP-10: System Recovery and Reconstitution IR-04: Incident Handling IR-08: Incident Response Plan	
	RC.RP-02: Recovery actions are selected, scoped, prioritized, and performed.	3	CP-10: System Recovery and Reconstitution IR-04: Incident Handling IR-08: Incident Response Plan	
	RC.CO-03: Recovery activities and progress in restoring operational capabilities are communicated to designated internal and external stakeholders.	3	IR-04: Incident Handling IR-06: Incident Reporting SR-08: Notification Agreements	
Mission Objective #2: Increase the Efficiency of the Transportation Ecosystem	GV.OC-03: Legal, regulatory, and contractual requirements regarding cybersecurity — including privacy and civil liberties obligations — are understood and managed.	3	Subcategory/Security Controls are covered in Mission Objective 1	
	GV.OC-04: Critical objectives, capabilities, and services that external	3	Subcategory/Security Controls are covered in Mission Objective 1	

Objectives	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
	stakeholders depend on or expect from the organization are understood and communicated.			
	ID.AM-01: Inventories of hardware managed by the organization are maintained.	3	Subcategory/Security Controls are covered in Mission Objective 1	
	ID.AM-02: Inventories of software, services, and systems managed by the organization are maintained.	3	Subcategory/Security Controls are covered in Mission Objective 1	
	ID.AM-03: Representations of the organization's authorized network communication and internal and external network data flows are maintained.	3	AC-04: Information Flow Enforcement CA-03: Information Exchange CA-09: Internal System Connections PL-02: System Security and Privacy Plans PL-08: Security and Privacy Architectures PM-07: Enterprise Architecture	PM-7 was not chosen because enterprise architecture planning is high-level and not applicable to individual DMS components. PL-08 was not chosen because system security architectures are defined at the overarching ITS architecture level (e.g., ARC-IT), not for individual DMS components, to maintain holistic integration.
	ID.AM-08: Systems, hardware, software, services, and data are	3	Subcategory/Security Controls are covered in Mission Objective 1	

Objectives	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
	managed throughout their lifecycles.			
	ID.IM-01: Improvements are identified from evaluations.	3	Subcategory/Security Controls are covered in Mission Objective 1	
	ID.IM-02: Improvements are identified from security tests and exercises, including those done in coordination with suppliers and relevant third parties.	3	Subcategory/Security Controls are covered in Mission Objective 1	
	ID.IM-04: Incident response plans and other cybersecurity plans that affect operations are established, communicated, maintained, and improved.	3	Subcategory/Security Controls are covered in Mission Objective 1	
	PR.AT-01: Personnel are provided with awareness and training so that they possess the knowledge and skills to perform general tasks with cybersecurity risks in mind.	3	Subcategory/Security Controls are covered in Mission Objective 1	
	PR.PS-03: Hardware is maintained, replaced, and	3	Subcategory/Security Controls are covered in Mission Objective 1	

Objectives	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
	removed commensurate with risk.			
	PR.IR-01: Networks and environments are protected from unauthorized logical access and usage.	3	AC-03: Access Enforcement AC-04: Information Flow Enforcement SC-04: Information In Shared System Resources SC-05: Denial-of-Service Protection SC-07: Boundary Protection	
	PR.IR-03: Mechanisms are implemented to achieve resilience requirements in normal and adverse situations.	3	Subcategory/Security Controls are covered in Mission Objective 1	
	RS.MA-01: The incident response plan is executed in coordination with relevant third parties once an incident is declared.	3	Subcategory/Security Controls are covered in Mission Objective 1	
	RS.MA-02: Incident reports are triaged and validated.	3	Subcategory/Security Controls are covered in Mission Objective 1	
	RS.MA-03: Incidents are categorized and prioritized.	3	Subcategory/Security Controls are covered in Mission Objective 1	
	RS.MA-04: Incidents are escalated or elevated as needed.	3	Subcategory/Security Controls are covered in Mission Objective 1	

Objectives	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
	RC.RP-05: The integrity of restored assets is verified, systems and services are restored, and normal operating status is confirmed.	3	CP-10: System Recovery and Reconstitution	
Mission Objective #3: Collect, Manage, Use, and Disseminate Data	GV.OC-02: Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered.	3	Subcategory/Security Controls are covered in Mission Objective 1	
	GV.OC-03: Legal, regulatory, and contractual requirements regarding cybersecurity — including privacy and civil liberties obligations — are understood and managed.	3	Subcategory/Security Controls are covered in Mission Objective 1	
	GV.OC-04: Critical objectives, capabilities, and services that external stakeholders depend on or expect from the organization are understood and communicated.	3	Subcategory/Security Controls are covered in Mission Objective 1	

Objectives	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
	GV.RM-03: Cybersecurity risk management activities and outcomes are included in enterprise risk management processes.	3	PM-03: Information Security and Privacy Resources PM-09: Risk Management Strategy PM-30: Supply Chain Risk Management Strategy RA-07: Risk Response SR-02: Supply Chain Risk Management Plan	
	GV.RM-05: Lines of communication across the organization are established for cybersecurity risks, including risks from suppliers and other third parties.	3	Subcategory/Security Controls are covered in Mission Objective 1	
	GV.SC-01: A cybersecurity supply chain risk management program, strategy, objectives, policies, and processes are established and agreed to by organizational stakeholders.	3	Subcategory/Security Controls are covered in Mission Objective 1	
	GV.SC-03: Cybersecurity supply chain risk management is integrated	3	Subcategory/Security Controls are covered in Mission Objective 1	

Objectives	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
	into .cybersecurity and enterprise risk management, risk assessment, and improvement processes.			
	GV.SC-04: Suppliers are known and prioritized by criticality.	3	Subcategory/Security Controls are covered in Mission Objective 1	
	GV.SC-05: Requirements to address cybersecurity risks in supply chains are established, prioritized, and integrated into contracts and other types of agreements with suppliers and other relevant third parties.	3	Subcategory/Security Controls are covered in Mission Objective 1	
	GV.SC-06: Planning and due diligence are performed to reduce risks before entering into formal supplier or other third-party relationships.	3	Subcategory/Security Controls are covered in Mission Objective 1	
	GV.SC-07: The risks posed by a supplier, their products and services, and other third parties are understood, recorded, prioritized, assessed,	3	Subcategory/Security Controls are covered in Mission Objective 1	

Objectives	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
	responded to, and monitored over the course of the relationship.			
	GV.SC-09: Supply chain security practices are integrated into cybersecurity and enterprise risk management programs, and their performance is monitored throughout the technology product and service lifecycle.	3	Subcategory/Security Controls are covered in Mission Objective 1	
	GV.SC-10: Cybersecurity supply chain risk management plans include provisions for activities that occur after the conclusion of a partnership or service agreement.	3	Subcategory/Security Controls are covered in Mission Objective 1	
	ID.AM-03: Representations of the organization's authorized network communication and internal and external network data flows are maintained.	3	Subcategory/Security Controls are covered in Mission Objective 2	
	ID.AM-07: Inventories of data and corresponding	3	CM-12: Information Location	CM-12 was not chosen because DMS operations involve fixed,

Objectives	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
	metadata for designated data types are maintained.		CM-13: Data Action Mapping SI-12: Information Management and Retention	known physical and logical locations in the field environment, making this control's focus on dynamically tracking and managing information locations unnecessary for a static roadway signage system.
	ID.AM-08: Systems, hardware, software, services, and data are managed throughout their lifecycles.	2	Subcategory/Security Controls are covered in Mission Objective 1 SC-28: Protecting of Information at Rest	Updated affinity score from 2 to 3 to appropriately amplifies the need for data management, aligning with the addition of SC-28 (Protecting of Information at Rest).
	ID.RA-01: Vulnerabilities in assets are identified, validated, and recorded.	3	CA-02: Control Assessments CA-07: Continuous Monitoring CA-08: Penetration Testing RA-03: Risk Assessment RA-05: Vulnerability Monitoring and Scanning SA-11(02): Threat Modeling and Vulnerability Analyses SA-15(07): Automated Vulnerability Analysis SA-15(08): Reuse of Threat and Vulnerability Information SI-04: System Monitoring	SI-5 was not chosen because processing security alerts is moderate priority but integrated into broader ITS monitoring rather than DMS-specific. SA-15(07) and (08) was not chosen because automated scanning tools are integrated into the central TMS vulnerability management process, not required on resource-constrained field DMS devices to optimize operational efficiency.

Objectives	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
			SI-05: Security Alerts, Advisories, and Directives	
	ID.RA-04: Potential impacts and likelihoods of threats exploiting vulnerabilities are identified and recorded.	3	Subcategory/Security Controls are covered in Mission Objective 1	
	ID.RA-05: Threats, vulnerabilities, likelihoods, and impacts are used to understand inherent risk and inform risk response prioritization.	3	Subcategory/Security Controls are covered in Mission Objective 1	
	ID.RA-10: Critical suppliers are assessed prior to acquisition.	3	Subcategory/Security Controls are covered in Mission Objective 1	
	ID.IM-03: Improvements are identified from execution of operational processes, procedures, and activities.	3	Subcategory/Security Controls are covered in Mission Objective 1	
	PR.AA-01: Identities and credentials for authorized users, services, and hardware are managed by the organization.	3	AC-01: Policy and Procedures AC-02: Account Management AC-14: Permitted Actions without Identification or Authentication IA-01: Policy and Procedures	IA-4 was not chosen because DMS systems have limited user accounts and identifiers, reducing the need for comprehensive management of identifiers in their operational context.

Objectives	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
			IA-02: Identification and Authentication (Organizational Users) IA-03: Device Identification and Authentication IA-04: Identifier Management IA-05: Authenticator Management IA-06: Authentication Feedback IA-07: Cryptographic Module Authentication IA-08: Identification and Authentication (Non-Organizational Users) IA-09: Service Identification and Authentication IA-10: Adaptive Authentication IA-11: Re-authentication	IA-05 was not chosen because DMS devices rely on system-level authentication for central TMS communications rather than individual user authenticators, as there are no direct human users interacting with the device in the field. IA-10 was not chosen because adaptive authentication is not applicable to DMS, as basic authentication mechanisms are covered in other controls.
	PR.AA-03: Users, services, and hardware are authenticated.	3	AC-07: Unsuccessful Logon Attempts AC-12: Session Termination IA-02: Identification and Authentication (Organizational Users) IA-03; Device Identification and Authentication IA-05: Authenticator Management IA-07: Cryptographic Module Authentication IA-08: Identification and Authentication (Non-Organizational Users)	

Objectives	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
			IA-09: Service Identification and Authentication IA-10: Adaptive Authentication IA-11: Re-authentication	
	PR.AA-05: Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties.	3	AC-01: Policy and Procedures AC-02: Account Management AC-03: Access Enforcement AC-05: Separation of Duties AC-06: Least Privilege AC-10: Concurrent Session Control AC-16: Security and Privacy Attributes AC-17: Remote Access AC-18: Wireless Access AC-24: Access Control Decisions IA-13: Identity Providers and Authorization Servers	IA-13 was not added to the list of security controls since it was withdrawn from NIST SP 800-53r5. ⁽¹⁾ Did not include AC-19: Access Control For Mobile Devices due to it's not being applicable to the DMS system.
	PR.AT-01: Personnel are provided with awareness and training so that they possess the knowledge and skills to perform general tasks with cybersecurity risks in mind.	3	Subcategory/Security Controls are covered in Mission Objective 1	

Objectives	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
	PR.DS-01: The C-I-A and availability of data-at-rest are protected.	3	CA-03: Information Exchange CP-09: System Backup MP-08: Media Downgrading SC-04: Information In Shared System Resources SC-07: Boundary Protection SC-12: Cryptographic Key Establishment and Management SC-13: Cryptographic Protection SC-28: Protection of Information At Rest SC-32: System Partitioning SC-39: Process Isolation SC-43: Usage Restrictions SI-03: Malicious Code Protection SI-04: System Monitoring SI-07: Software, Firmware, and Information Integrity	MP-8 was not chosen because media downgrading is irrelevant for DMS systems, as they do not handle classified or sensitive media requiring sanitization processes. SC-12 was not chosen because key management for DMS encryption is handled by the central TMS or network infrastructure, not locally on the device, to centralize cryptographic operations and reduce field complexity. SC-16 was not chosen because DMS transmissions include only essential operational attributes (e.g., status and messages) without privacy-sensitive metadata, making attribute-specific protections unnecessary. SC-32 was not chosen because system partitioning is less relevant for DMS, which have simple architectures without complex internal divisions.
	PR.DS-02: The C-I-A of data-in-transit are protected.	3	AU-16: Cross-Organizational Audit Logging CA-03: Information Exchange	

Objectives	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
			SC-04: Information In Shared System Resources SC-07: Boundary Protection SC-08: Transmission Confidentiality and Integrity SC-11: Trusted Path SC-12: Cryptographic Key Establishment and Management SC-13: Cryptographic Protection SC-16: Transmission of Security and Privacy Attributes SC-40: Wireless Link Protection SC-43: Usage Restrictions SI-03: Malicious Code Protection SI-04: System Monitoring SI-07: Software, Firmware, and Information Integrity	
	PR.DS-10: The C-I-A of data-in-use are protected.	3	AC-02: Account Management AC-03: Access Enforcement AC-04: Information Flow Enforcement AU-09: Protection of Audit Information AU-13: Monitoring For Information Disclosure CA-03: Information Exchange CP-09: System Backup	

Objectives	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
			SA-08: Security and Privacy Engineering Principles SC-04: Information In Shared System Resources SC-07: Boundary Protection SC-11: Trusted Path SC-13: Cryptographic Protection SC-24: Fail In Known State SC-32: System Partitioning SC-39: Process Isolation SC-40: Wireless Link Protection SC-43: Usage Restrictions SI-03: Malicious Code Protection SI-04: System Monitoring SI-07: Software, Firmware, and Information Integrity SI-10: Information Input Validation SI-16: Memory Protection	
	PR.DS-11: Backups of data are created, protected, maintained, and tested.	3	CP-06: Alternate Storage Site CP-09: System Backup	
	PR.PS-02: Software is maintained, replaced, and removed commensurate with risk.	2	CM-11: User-Installed Software MA-03(06): Software Updates and Patches	

Objectives	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
			SA-10(01): Software and Firmware Integrity Verification SI-02: Flaw Remediation SI-07: Software, Firmware, and Information Integrity	
	PR.PS-04: Log records are generated and made available for continuous monitoring.	3	AU-02: Event Logging AU-03: Content of Audit Records AU-06: Audit Record Review, Analysis, and Reporting AU-07: Audit Record Reduction and Report Generation AU-11: Audit Record Retention AU-12: Audit Record Generation	PS-4 was not chosen because personnel termination procedures are organizational and irrelevant for DMS with limited access points.
	PR.IR-01: Networks and environments are protected from unauthorized logical access and usage.	3	Subcategory/Security Controls are covered in Mission Objective 2	IR-01 was not chosen because incident response policies and procedures are managed at the broader ITS or TMS level, not tailored to individual DMS devices to streamline enterprise-wide consistency.
	PR.IR-03: Mechanisms are implemented to achieve resilience requirements in normal and adverse situations.	3	Subcategory/Security Controls are covered in Mission Objective 1	
	PR.IR-04: Adequate resource capacity to	2	Subcategory/Security Controls are covered in Mission Objective 1	

Objectives	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
	ensure availability is maintained.			
	DE.CM-09: Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events.	2	AC-04: Information Flow Enforcement AC-09: Previous Logon Notification AU-12: Audit Record Generation CA-07: Continuous Monitoring CM-03: Configuration Change Control CM-06: Configuration Settings CM-10: Software Usage Restrictions CM-11: User-Installed Software SC-34: Non-Modifiable Executable Programs SC-35: External Malicious Code Identification SI-04: System Monitoring SI-07: Software, Firmware, and Information Integrity	CM-10 was not chosen because DMS typically uses proprietary, pre-approved software with minimal need for restrictions on user-installed applications in their controlled field deployment.
	RS.MA-01: The incident response plan is executed in coordination with relevant third parties once an incident is declared.	3	Subcategory/Security Controls are covered in Mission Objective 1	
	RS.MA-04: Incidents are escalated or elevated as needed.	3	Subcategory/Security Controls are covered in Mission Objective 1	
	RS.AN-07: Incident data and metadata are	3	Subcategory/Security Controls are covered in Mission Objective 1	

U.S. Department of Transportation
Office of the Assistant Secretary for Research and Technology
Intelligent Transportation Systems Joint Program Office

Objectives	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
	collected, and their integrity and provenance are preserved.			
	RC.RP-01: The recovery portion of the incident response plan is executed once initiated from the incident response process.	3	Subcategory/Security Controls are covered in Mission Objective 1	
	RC.RP-02: Recovery actions are selected, scoped, prioritized, and performed.	3	Subcategory/Security Controls are covered in Mission Objective 1	
	RC.RP-03: The integrity of backups and other restoration assets is verified before using them for restoration.	3	CP-02: Contingency Plan CP-04: Contingency Plan Testing CP-09: System Backup	
	RC.RP-04: Critical mission functions and cybersecurity risk management are considered to establish post-incident operational norms.	3	PM-08: Critical Infrastructure Plan PM-09: Risk Management Strategy PM-11: Mission and Business Process Definition IR-01: Policy and Procedures IR-08: Incident Response Plan	
	RC.RP-05: The integrity of restored assets is verified, systems and services are restored, and normal	3	Subcategory/Security Controls are covered in Mission Objective 2	

Objectives	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
	operating status is confirmed.			
Mission Objective #8: Build Privacy Protections into ITS Operations	GV.OC-02: Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered.	3	Subcategory/Security Controls are covered in Mission Objective 1	
	GV.OC-03: Legal, regulatory, and contractual requirements regarding cybersecurity — including privacy and civil liberties obligations — are understood and managed.	3	Subcategory/Security Controls are covered in Mission Objective 3	
	GV.RM-03: Cybersecurity risk management activities and outcomes are included in enterprise risk management processes.	3	Subcategory/Security Controls are covered in Mission Objective 3	
	GV.RR-02: Roles, responsibilities, and authorities related to cybersecurity risk management are established,	3	PM-02: Information Security Program Leadership Role PM-13: Security and Privacy Workforce PM-19: Privacy Program Leadership Role PM-23: Data Governance Body	PM-13 was not chosen because workforce management for security and privacy are organizational-level and less critical for the operational focus of DMS field devices.

U.S. Department of Transportation
Office of the Assistant Secretary for Research and Technology
Intelligent Transportation Systems Joint Program Office

Objectives	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
	communicated, understood, and enforced.		PM-24: Data Integrity Board PM-29: Risk Management Program Leadership Roles	
	GV.PO-01: Policy for managing cybersecurity risks is established based on organizational context, cybersecurity strategy, and priorities and is communicated and enforced.	3	AC-01: Policy and Procedures AT-01: Policy and Procedures AU-01: Policy and Procedures CA-01: Policy and Procedures CM-01: Policy and Procedures CP-01: Policy and Procedures IA-01: Policy and Procedures IR-01: Policy and Procedures MA-01: Policy and Procedures MP-01: Policy and Procedures PE-01: Policy and Procedures PL-01: Policy and Procedures PM-01: Information Security Program Plan PS-01: Policy and Procedures PT-01: Policy and Procedures RA-01: Policy and Procedures SA-01: Policy and Procedures SC-01: Policy and Procedures SI-01: Policy and Procedures SR-01: Policy and Procedures	

Objectives	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
	GV.PO-02: Policy for managing cybersecurity risks is reviewed, updated, communicated, and enforced to reflect changes in requirements, threats, technology, and organizational mission.	3	Same controls as GV.PO-01	
	GV.SC-02: Cybersecurity roles and responsibilities for suppliers, customers, and partners are established, communicated, and coordinated internally and externally.	3	SR-02: Supply Chain Risk Management Plan SR-03: Supply Chain Controls and Processes SR-05: Acquisition Strategies, Tools, and Methods	
	ID.AM-04: Inventories of services provided by suppliers are maintained.	3	AC-20: Use of External Systems SA-09: External System Services SR-02: Supply Chain Risk Management Plan	
	ID.AM-07: Inventories of data and corresponding metadata for designated data types are maintained.	3	Subcategory/Security Controls are covered in Mission Objective 3	
	ID.AM-08: Systems, hardware, software, services, and data are managed throughout their lifecycles.	3	Subcategory/Security Controls are covered in Mission Objective 1	

U.S. Department of Transportation
Office of the Assistant Secretary for Research and Technology
Intelligent Transportation Systems Joint Program Office

Objectives	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
	ID.RA-01: Vulnerabilities in assets are identified, validated, and recorded.	3	Subcategory/Security Controls are covered in Mission Objective 3	
	ID.RA-04: Potential impacts and likelihoods of threats exploiting vulnerabilities are identified and recorded.	3	Subcategory/Security Controls are covered in Mission Objective 1	
	ID.RA-05: Threats, vulnerabilities, likelihoods, and impacts are used to understand inherent risk and inform risk response prioritization.	3	Subcategory/Security Controls are covered in Mission Objective 1	
	ID.RA-06: Risk responses are chosen, prioritized, planned, tracked, and communicated.	3	Subcategory/Security Controls are covered in Mission Objective 1	
	PR.AA-01: Identities and credentials for authorized users, services, and hardware are managed by the organization.	3	Subcategory/Security Controls are covered in Mission Objective 3	
	PR.AA-03: Users, services, and hardware are authenticated.	3	Subcategory/Security Controls are covered in Mission Objective 3	

Objectives	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
	PR.AA-04: Identity assertions are protected, conveyed, and verified.	3		
	PR.AA-05: Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties.	3	Subcategory/Security Controls are covered in Mission Objective 3	
	PR.AT-01: Personnel are provided with awareness and training so that they possess the knowledge and skills to perform general tasks with cybersecurity risks in mind.	3	Subcategory/Security Controls are covered in Mission Objective 3	
	PR.DS-01: C-I-A of data-at-rest are protected.	3	Subcategory/Security Controls are covered in Mission Objective 3	
	PR.DS-02: C-I-A of data-in-transit are protected.	3	Subcategory/Security Controls are covered in Mission Objective 3	
	PR.DS-10: C-I-A of data-in-use are protected.	3	AC-02: Account Management AC-03: Access Enforcement AC-04: Information Flow Enforcement AU-09: Protection of Audit Information	

U.S. Department of Transportation
Office of the Assistant Secretary for Research and Technology
Intelligent Transportation Systems Joint Program Office

Objectives	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
			AU-13: Monitoring For Information Disclosure CA-03: Information Exchange CP-09: System Backup SA-08: Security and Privacy Engineering Principles SC-04: Information In Shared System Resources SC-07: Boundary Protection SC-11: Trusted Path SC-13: Cryptographic Protection SC-24: Fail In Known State SC-32: System Partitioning SC-39: Process Isolation SC-40: Wireless Link Protection SC-43: Usage Restrictions SI-03: Malicious Code Protection SI-04: System Monitoring SI-07: Software, Firmware, and Information Integrity SI-10: Information Input Validation SI-16: Memory Protection	
	PR.IR-01: Networks and environments are protected from	3	Subcategory/Security Controls are covered in Mission Objective 3	

Objectives	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
	unauthorized logical access and usage.			
	DE.CM-01: Networks and network services are monitored to find potentially adverse events.	3	Subcategory/Security Controls are covered in Mission Objective 1	
	DE.CM-03: Personnel activity and technology usage are monitored to find potentially adverse events.	3	AC-02: Account Management AU-12: Audit Record Generation AU-13: Monitoring For Information Disclosure CA-07: Continuous Monitoring CM-10: Software Usage Restrictions CM-11: User-Installed Software	
	DE.CM-06: External service provider activities and services are monitored to find potentially adverse events.	3	CA-07: Continuous Monitoring PS-07: External Personnel Security SA-04: Acquisition Process SA-09: External System Services SI-04: System Monitoring	
	RS.AN-07: Incident data and metadata are collected, and their integrity and provenance are preserved.	3	AU-07: Audit Record Reduction and Report Generation IR-04: Incident Handling IR-06: Incident Reporting	
	RS.MI-01: Incidents are contained.	3	Subcategory/Security Controls are covered in Mission Objective 1	

Objectives	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
	RS.MI-02: Incidents are eradicated.	3	Subcategory/Security Controls are covered in Mission Objective 1	
Mission Objective #11: Enhance Telecommunications and Networking to Facilitate Emerging ITS Capabilities	GV.RM-07: Strategic opportunities (i.e., positive risks) are characterized and are included in organizational cybersecurity risk discussions.	3	Subcategory/Security Controls are covered in Mission Objective 1	
	GV.RR-02: Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced.	3	Subcategory/Security Controls are covered in Mission Objective 8	
	GV.OV-01: Cybersecurity risk management strategy outcomes are reviewed to inform and adjust strategy and direction.	3	Subcategory/Security Controls are covered in Mission Objective 1	
	GV.OV-02: The cybersecurity risk management strategy is reviewed and adjusted to ensure coverage of	3	PM-09: Risk Management Strategy PM-18: Privacy Program Plan PM-30: Supply Chain Risk Management Strategy SR-03: Supply Chain Controls and Processes	

Objectives	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
	organizational requirements and risks.		SR-05: Acquisition Strategies, Tools, and Methods SR-06: Supplier Assessments and Reviews SR-08: Notification Agreements	
	GV.OV-03: Organizational cybersecurity risk management performance is evaluated and reviewed for adjustments needed.	3	AC-01 Policy and Procedures AT-01 Policy and Procedures AU-01 Policy and Procedures CA-01 Policy and Procedures CM-01 Policy and Procedures CP-01: Policy and Procedures IA-01: Policy and Procedures IR-01: Policy and Procedures MA-01: Policy and Procedures MP-01: Policy and Procedures PE-01: Policy and Procedures PL-01: Policy and Procedures PM-01: Information Security Program Plan PS-01: Policy and Procedures PT-01: Policy and Procedures RA-01: Policy and Procedures SA-01: Policy and Procedures SC-01: Policy and Procedures SI-01: Policy and Procedures SR-01: Policy and Procedures	

Objectives	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
			PM-28: Risk Framing	
	GV.SC-02: Cybersecurity roles and responsibilities for suppliers, customers, and partners are established, communicated, and coordinated internally and externally.	3	Subcategory/Security Controls are covered in Mission Objective 8	
	ID.AM-01: Inventories of hardware managed by the organization are maintained.	3	Subcategory/Security Controls are covered in Mission Objective 1	
	ID.AM-02: Inventories of software, services, and systems managed by the organization are maintained.	3	Subcategory/Security Controls are covered in Mission Objective 1	
	ID.AM-03: Representations of the organization's authorized network communication and internal and external network data flows are maintained.	3	Subcategory/Security Controls are covered in Mission Objective 3	

Objectives	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
	ID.AM-04: Inventories of services provided by suppliers are maintained.	3	Subcategory/Security Controls are covered in Mission Objective 8	
	ID.AM-05: Assets are prioritized based on classification, criticality, resources, and impact on the mission.	3	RA-03: Risk Assessment RA-09: Criticality Analysis RA-02: Security Categorization	RA-02 was not chosen because security categorization of the overall ITS system, including DMS, is performed at the program level rather than per device to align with federal categorization standards.
	ID.AM-07: Inventories of data and corresponding metadata for designated data types are maintained.	3	Subcategory/Security Controls are covered in Mission Objective 3	
	ID.RA-07: Changes and exceptions are managed, assessed for risk impact, recorded, and tracked.	3	CA-07: Continuous Monitoring CM-03: Configuration Change Control CM-04: Impact Analyses	
	ID.IM-01: Improvements are identified from evaluations.	3	Subcategory/Security Controls are covered in Mission Objective 1	
	ID.IM-04: Incident response plans and other cybersecurity plans that affect operations are established, communicated, maintained, and improved.	3	Subcategory/Security Controls are covered in Mission Objective 1	

Objectives	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
	PR.AA-04: Identity assertions are protected, conveyed, and verified.	3	Subcategory/Security Controls are covered in Mission Objective 8	
	PR.DS-01: C-I-A of data-at-rest are protected.	3	Subcategory/Security Controls are covered in Mission Objective 3	
	PR.DS-02: C-I-A of data-in-transit are protected.	3	Subcategory/Security Controls are covered in Mission Objective 3	
	PR.PS-01: Configuration management practices are established and applied.	3	CM-01: Policy and Procedures CM-02: Baseline Configuration CM-03: Configuration Change Control CM-04: Impact Analyses CM-05: Access Restrictions For Change CM-06: Configuration Settings CM-07: Least Functionality CM-08: System Component Inventory CM-09: Configuration Management Plan CM-10: Software Usage Restrictions CM-11: User-Installed Software	
	PR.PS-04: Log records are generated and made available for continuous monitoring.	3	Subcategory/Security Controls are covered in Mission Objective 3	
	PR.IR-01: Networks and environments are	3	Subcategory/Security Controls are covered in Mission Objective 3	

Objectives	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
	protected from unauthorized logical access and usage.			
	PR.IR-03: Mechanisms are implemented to achieve resilience requirements in normal and adverse situations.	3	Subcategory/Security Controls are covered in Mission Objective 1	
	DE.CM-01: Networks and network services are monitored to find potentially adverse events.	3	Subcategory/Security Controls are covered in Mission Objective 1	

Appendix C. Abbreviations

ARC-IT	Architecture Reference for Cooperative and Intelligent Transportation
ATMS	advanced transportation management system
CAV	connected automated vehicle
C-I-A	confidentiality, integrity, and availability
CISA	Cybersecurity and Infrastructure Security Agency
CSF	Cybersecurity Framework
CVO	Commercial Vehicle Operations
DMS	dynamic message sign
DoS	denial of service
EMP	electromagnetic pulse
FHWA	Federal Highway Administration
FIPS	Federal Information Processing Standard
FTP	File Transfer Protocol
G	guidance
I	IOO
ICS	industrial control system
IDS	intrusion detection system
IEEE	Institute of Electrical and Electronics Engineers
IOO	infrastructure owner/operator
IP	Internet protocol
IPS	intrusion protection system
IPSec	Internet protocol security
ITS	intelligent transportation system
L-M-H	low-moderate-high
M	manufacturer
M/I	manufacturer/IOO
NIST	National Institute of Standards and Technology
NS	not selected

NTCIP	National Transportation Communications for ITS Protocol
OT	operational technology
PLC	programmable logic controller
POLP	principle of least privilege
R	risk
RFC	request for comment
S	standard
SCADA	Supervisory Control and Data Acquisition
TCP	Transmission Control Protocol
TLS	transport layer security
TMC	traffic management center
TMS	traffic management system
UDP	user datagram protocol
V	value
VLAN	virtual local area network
Wi-Fi	wireless fidelity

Appendix D. Control Family Abbreviations

AC	Access Control
AT	Awareness and Training
AU	Audit and Accountability
CA	Assessment, Authorization, and Monitoring
CM	Configuration Management
CP	Contingency Planning
IA	Identification and Authentication
IR	Incident Response
MA	Maintenance
MP	Media Protection
PE	Physical and Environmental Protection
PM	Program Management
PL	Planning
RA	Risk Assessment
SA	System and Services Acquisition
SC	System and Communications Protection
SI	System and Information Integrity
SR	Supply Chain Risk Management

Appendix E. Glossary

CAV infrastructure system	Systems deployed by departments of transportation to enable communication between roadside infrastructure and onboard units within CAVs. These systems facilitate the exchange of information flows, such as traffic conditions or advisories, and may interface with DMS or DMS control software to provide consistent messaging to both CAVs and human drivers.
connected vehicle	A vehicle connected device that is equipped with onboard equipment that is active and operational and includes the means to send and receive data to and from other connected devices.
device security class	A statement of the security requirements for a device in terms of its requirements for C-I-A, expressed as L-M-H ratings for each of the three.
DMS controller	A device that controls and monitors the operations of a DMS. It manages sign functions, such as message display and status reporting, and supports multiple control interfaces, including local control panels, local field programming terminals, or central computers. The DMS controller ensures reliable operation of the sign and facilitates communication with DMS control software or other transportation management systems, contributing to the functionality of the ITS.
enterprise object	An organization or individual that interacts with other enterprise objects and/or physical objects. An enterprise object may be a component of another larger enterprise object, which may in turn be a component of a third, even larger, enterprise object (e.g., a TMC manager is a component of State government). Enterprise objects may participate wholly or in part in other enterprise objects (e.g., a device developer is a component of auto manufacturer but also participates in standards body).
field	Infrastructure proximate to the transportation network which performs surveillance (e.g., traffic detectors, cameras), traffic control (e.g., signal controllers), information provision (e.g., DMS and local transaction (e.g., tolling, parking) functions. Typically governed by transportation management functions running in centers. Field also includes connected vehicle roadside equipment and other non-dedicated short-range communications wireless communications infrastructure that provides communications between mobile elements and fixed infrastructure.

field programming terminal	A portable computer running maintenance software designed to interface with a DMS controller. It enables technicians to perform diagnostics, configure sign settings, and control sign activation locally. The field programming terminal supports maintenance and troubleshooting of DMS operations.
information	flow Information that is exchanged between physical objects (subsystems and terminators) in the physical view of ARC-IT. The terms information flow and architecture flow are used interchangeably. Information flows are the primary tool that is used to define the ITS architecture interfaces. These information flows and their communication requirements define the interfaces which form the basis for much of the ongoing standards work in the national ITS program.
intelligent transportation system	The system defined as the electronics, communications, or information processing in transportation infrastructure and in vehicles used singly or integrated to improve transportation safety and mobility and enhance productivity. Intelligent transportation systems encompass a broad range of wireless and wire line communications-based information and electronics technologies.
onboard equipment	Computer modules, display, and a dedicated short-range communications radio, that is installed and embedded into vehicles which provide an interface to vehicular sensors, as well as a wireless communication interface to the roadside and back-office environment.
physical object	Systems or devices that provide ITS functionality that makes up the ITS and the surrounding environment. They are defined in terms of the services they support, the processing they include, and their interfaces with other physical objects. They are grouped into six classes: centers, field, ITS, support, travelers, and vehicles. Example physical objects are the TMC, the vehicle onboard equipment, and the ITS roadway equipment. These correspond to the physical world: respectively traffic operations centers, equipped connected automobiles, and roadside signal controllers. Due to this close correspondence between the physical world and the physical objects, the interfaces between them are prime candidates for standardization. In ARC-IT, physical objects are defined with scope such that they are under the control of a single enterprise object.
risk tolerance	The organization's or stakeholder's readiness to bear the risk after risk treatment in order to achieve its objectives. Risk tolerance can be influenced by legal or regulatory requirements.

security control	Safeguards or countermeasures prescribed for a system or an organization to protect the C-I-A of the system and its information.
service package	Provides an accessible, service-oriented perspective to ARC-IT and is tailored to fit, separately or in combination, real world transportation problems and needs. Service packages collect one or more functional objects that must work together to deliver a given ITS service and the information flows that connect them and other important external systems. In other words, they identify the pieces of the physical view that are required to implement a particular ITS service. Service packages are implemented through projects (or groups of projects, aka programs) and in transportation planning, are directly related to ITS strategies used to meet regional goals and objectives.

References

1. National Institute of Standards and Technology. 2020. *Security and Privacy Controls for Information Systems and Organizations*. NIST SP 800-53 Rev. 5. Washington, DC. U.S. Department of Commerce. September 2020 (includes updates as of December 10, 2020). <https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final>, last accessed October 15, 2025.
2. National Institute of Standards and Technology. 2017. *Digital Identity Guidelines – Authentication and Lifecycle Management*. NIST SP 800-63B (superseded). Published June 2017 (includes updates as of March 2, 2020). <https://pages.nist.gov/800-63-3/sp800-63b.html>, last accessed October 10, 2025.
3. National Institute of Standards and Technology. 2015. Guide to Industrial Control Systems (ICS) Security. NIST SP 800-82 Rev. 2 (superseded). Published May 2015. <https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final>, last accessed October 15, 2025.
4. National Institute of Standards and Technology. 2024. The NIST Cybersecurity Framework (CSF) 2.0. Washington, DC. U.S. Department of Commerce. <https://doi.org/10.6028/NIST.CSWP.29>, last accessed October 10, 2025.
5. National Transportation Communications for Intelligent Transportation System Protocol. 2014. Object Definitions for Dynamic Message Signs (DMS). NTCIP 1203 v. 03. Published September 2014. Washington, DC. U.S. <https://www.ntcip.org/file/2018/11/NTCIP1203v03f.pdf>, last accessed February 20, 2026.
6. Federal Highway Administration. 2018. Model Systems Engineering Documents for Dynamic Message Sign (DMS) Systems. Published September 2018. <https://ops.fhwa.dot.gov/publications/fhwahop18080/fhwahop18080.pdf>, last accessed February 20, 2026.
7. International Telecommunication Union (ITU). 2023. *X.509: Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks*. Published November 25, 1988; updated October 29, 2023.
8. National Institute of Standards and Technology. 2019. *Security Requirements for Cryptographic Modules*. Federal Information Processing Standard Publication FIPS PUB 140-3. Issued March 22, 2019. Washington, DC. U.S. Department of Commerce. <https://csrc.nist.gov/publications/detail/fips/140/3/final>, last accessed October 10, 2025.
9. Cybersecurity & Infrastructure Security Agency. n.d. “Cybersecurity Alerts & Advisories” (web page). <https://www.cisa.gov/news-events/cybersecurity-advisories>, last accessed October 10, 2025.
10. National Institute of Standards and Technology. n.d. National Vulnerability Database. <https://nvd.nist.gov/>, last accessed October 10, 2025.
11. OWASP® Foundation. n.d. “OWASP® Top Ten” (website). Open Worldwide Application Security Project. <https://owasp.org/www-project-top-ten/>, last accessed October 10, 2025.

12. Cybersecurity & Infrastructure Security Agency. n.d. Known Exploited Vulnerabilities Catalog. <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>, last accessed October 10, 2025.
13. The Supervisory Control and Data Acquisition (SCADA)/Control Systems Procurement Project. n.d. ICS Recommended Practices <https://www.cisa.gov/resources-tools/resources/ics-recommended-practices>, last accessed November 3, 2025.
14. National Institute of Standards and Technology. 2022. *Validating the Integrity of Computing Devices*. NIST SP 1800-34. Published December 2022. <https://csrc.nist.gov/pubs/sp/1800/34/final>, last accessed October 14, 2025.
15. Institute of Electrical and Electronics Engineers. 2022. *Standard for Ethernet*. IEEE Standard 802.3-2022. Published July 29, 2022. <https://standards.ieee.org/ieee/802.3/10422/>, last accessed October 14, 2025.
16. National Institute of Standards and Technology. 2015. *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*. NIST SP 800-90A Rev. 1. Published June 2015. Washington, DC. U.S. Department of Commerce. <https://csrc.nist.gov/pubs/sp/800/90/a/r1/final>, last accessed October 14, 2025.
17. National Institute of Standards and Technology. *Advanced Encryption Standard (AES)*. Federal Information Processing Standards Publication. FIPS 197. Published November 26, 2001; updated May 9, 2023. Washington, DC. U.S. Department of Commerce. <https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.197.pdf>, last accessed October 14, 2025.
18. ARC-IT Version 9.3. n.d. "Notes on Access Control." <https://www.arc-it.net/html/security/controlsclarification.html>, last accessed October 14, 2025.
19. National Institute of Standards and Technology. 2011. *BIOS Protection Guidelines*. NIST SP 800-147. Published April 2011. Washington, DC. U.S. Department of Commerce. <https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-147.pdf>, last accessed October 14, 2025.
20. National Institute of Standards and Technology. 2007. *Guide to Storage Encryption Technologies for End User Devices*. NIST SP 800-111. Published November 2007. Washington, DC. U.S. Department of Commerce. <https://csrc.nist.gov/pubs/sp/800/111/final>, last accessed November 4, 2025.
21. National Institute of Standards and Technology. 2020. *Recommendation for Key Management: Part 1 – General*. NIST SP 800-57 Part Rev. 5. Published May 2020. Washington, DC. U.S. Department of Commerce. <https://csrc.nist.gov/pubs/sp/800/57/pt1/r5/final>, last accessed November 4, 2025.
22. National Institute of Standards and Technology. 2008. *Technical Guide to Information Security Testing and Assessment*. NIST SP 800-115. Published September 2008. Washington, DC. U.S. Department of Commerce. <https://csrc.nist.gov/pubs/sp/800/115/final>, last accessed November 4, 2025.
23. National Institute of Standards and Technology. 2018. *Platform Firmware Resiliency Guidelines*. NIST SP 800-193. Published May 2018. Washington, DC. U.S. Department of Commerce. <https://csrc.nist.gov/pubs/sp/800/193/final>, last accessed November 4, 2025.

24. National Institute of Standards and Technology. 2011. *BIOS Protection Guidelines*. NIST SP 800-147. Published April 2011. Washington, DC. U.S. Department of Commerce. <https://csrc.nist.gov/pubs/sp/800/147/final>, last accessed November 4, 2025
25. National Institute of Standards and Technology. 2022. *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*. NIST SP 800-161 Rev 1. Published May 2022. Washington, DC. U.S. Department of Commerce. <https://csrc.nist.gov/pubs/sp/800/161/r1/upd1/final>, last accessed November 4, 2025.
26. International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC). 2015. *Information technology — Trusted platform module library Part 1: Architecture*. ISO/IEC 11889-1:2015, published August 2015. <https://www.iso.org/standard/66510.html>, last accessed November 4, 2025.
27. International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC). 2025. *Information security, cybersecurity and privacy protection — Security requirements for cryptographic modules*. ISO/IEC 19790:2025, published February 2025. <https://www.iso.org/standard/82423.html>, last accessed November 4, 2025
28. International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC). 2010. *Information technology — Security techniques — Encryption algorithms Part 3: Block ciphers* ISO/IEC 18033-3-1:2010, published December 2010. <https://www.iso.org/standard/54531.html>, last accessed November 4, 2025.
29. National Institute of Standards and Technology. 2019. *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations*. NIST SP 800-52. Washington, DC. U.S. Department of Commerce. August 2019 (includes updates as of December 10, 2020). <https://csrc.nist.gov/pubs/sp/800/52/r2/final>, last accessed November 4, 2025.
30. National Institute of Standards and Technology. 2016. *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security*. NIST SP 800-46 Rev 2. Published July 2016. Washington, DC. U.S. Department of Commerce. <https://csrc.nist.gov/pubs/sp/800/46/r2/final>, last accessed November 4, 2025.
31. International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC). 2022. *Information security, cybersecurity and privacy protection — Information security controls*. ISO/IEC 27002:2022, published February 2022. <https://www.iso.org/standard/82423.html>, last accessed November 4, 2025
32. National Institute of Standards and Technology. 2024. *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*. NIST SP 800-171 Rev. 3. Published May 2024. Washington, DC. U.S. Department of Commerce. <https://csrc.nist.gov/pubs/sp/800/171/r3/final>, last accessed November 4, 2025.
33. National Institute of Standards and Technology. 2018. *Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography*. NIST SP 800-56A Rev. 3. Published April 2018. Washington, DC. U.S. Department of Commerce. <https://csrc.nist.gov/pubs/sp/800/56/a/r3/final>, last accessed November 4, 2025.
34. The MITRE Corporation. 2025. MITRE ATT&CK v17.1. Bedford, Massachusetts, and McLean, Virginia. <https://attack.mitre.org/versions/v17/>, last accessed October 10, 2025.

35. National Institute of Standards and Technology. 2012. Guide for Conducting Risk Assessments. NIST SP 800-30 Rev. 1. Washington, DC. U.S. Department of Commerce. September 2012. <https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final>, last accessed October 15, 2025
36. Internet Engineering Task Force (IETF). 2018. The Transport Layer Security (TLS) Protocol Version 1.3. Request for Comment 8446. RFC Editor. August 2018. <https://www.rfc-editor.org/rfc/rfc8446>, last accessed October 15, 2025
37. Institute of Electrical and Electronics Engineers (IEEE). 2020. IEEE Standard for Local and Metropolitan Area Networks--Port-Based Network Access Control. IEEE Standard 802.1X-2020, published February 2020. <https://standards.ieee.org/ieee/802.1X/7345/>, last accessed November 4, 2025
38. Institute of Electrical and Electronics Engineers (IEEE). 2024. IEEE Standard for Information technology--Telecommunications and information exchange between systems Local and metropolitan area networks--Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. IEEE 802.11-2024. Published April 28, 2025. <https://standards.ieee.org/ieee/802.11/5536/>, last accessed October 14, 2025
39. National Transportation Communications for ITS Protocol. 2021. Infrastructure Standards Security Assessment (ISSA). NTCIP 9014 v01.20. Published August 2021. American Association of State Highway and Transportation Officials (AASHTO), Institute of Transportation Engineers (ITE), and National Electrical Manufacturers Association (NEMA). <https://www.ntcip.org/file/2021/08/NTCIP9014v0120.pdf>, last accessed October 15, 2025
40. National Institute of Standards and Technology. 2018. Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. NIST SP 800-37 Rev. 2. Washington, DC. U.S. Department of Commerce. <https://csrc.nist.gov/pubs/sp/800/37/r2/final>, last accessed October 15, 2025

U.S. Department of Transportation
ITS Joint Program Office – HOIT
1200 New Jersey Avenue, SE
Washington, DC 20590
Toll-Free “Help Line” 866-367-7487
www.its.dot.gov

FHWA-JPO-26-004



U.S. Department of Transportation