

Intelligent Transportation Systems (ITS) Security Control Set for Roadside Units

www.its.dot.gov/index.htm

Final Report – April 2026
FHWA-JPO-26-003



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-26-003		2. Government Accession No.		3. Recipient's Catalog No.	
4. Title and Subtitle Intelligent Transportation Systems (ITS) Security Control Set for Roadside Units				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 manager is Joe Gregory.					
16. Abstract This control set document identifies security controls typically needed to mitigate security risks to roadside units (RSUs) operating in the role of connected vehicle roadside equipment described in the Architecture Reference for Cooperative and Intelligent Transportation (ARC-IT). The objective of this control set is to provide a means to better protect RSUs and the information flows supported by their interfaces as more advanced features are added. The controls (primarily technical controls) relevant to RSUs 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 240	
				22. Price	

Table of Contents

Chapter 1. Identification.....	1
Purpose, Scope, and Applicability	1
Revisions	2
Sources	2
Relationship between ARC-IT, CSF, and Control Sets	3
Chapter 2. Physical Object Characteristics.....	5
Definition/Description	5
Physical Object Device Security Class by Service Package	8
Assumptions and Characteristics.....	11
Resources for Identifying Threats, Vulnerabilities, and Predisposing Conditions	13
Connection Between the ITS Profile, CSF Subfunctions, and NIST SP 800-53 Controls.....	13
Chapter 3. Summary of Control Specifications	15
Chapter 4. Detailed Control Specifications	31
AC Family – Access Control.....	32
AT Family – Awareness and Training.....	57
AU Family – Audit and Accountability	58
CA Family – Assessment, Authorization, and Monitoring	68
CM Family – Configuration Management.....	74
CP Family – Contingency Planning	81
IA Family – Identification and Authentication	83
IR Family – Incident Response	92
MA Family – Maintenance	94
PE Family – Physical and Environmental Protection	96
PL Family – Planning	101
PM Family – Program Management.....	102
RA Family – Risk Assessment.....	102
SA Family – System and Services Acquisition	106
SC Family – System and Communications Protection	113
SI FAMILY – SYSTEM AND INFORMATION INTEGRITY	132
SR Family – Supply Chain Risk Management.....	142

Chapter 5. Implementation Considerations	145
Organizations should consider the following control guidance when implementing RSUs that store, process, or transmit ITS information. These considerations focus on exposed roadside deployment environments, embedded firmware integrity, cryptographic trust, and V2X certificate management.	145
AC-3(2), Access Enforcement Dual Authorization.....	145
AC-6(8), Least Privilege Privilege Levels for Code Execution(1), (8), (10).....	145
CM-2, Baseline Configuration	146
PE-3, Physical Access Control.....	146
SA-10, Develop Configuration Management	146
SI-3, Malicious Code Protection	146
SI-7(1), Software, Firmware, and Information Integrity Integrity Checks (1,2,6,9,10,12).....	146
SR-9, Tamper Resistance and Detection.....	148
Appendix A. Threats, Vulnerabilities and Predisposing Conditions	149
Appendix B. NIST SP 800-53 Security Control's Mapping.....	161
Appendix C. Acronyms	219
Appendix D. Control Family Abbreviations	221
Appendix E. Glossary	223
References.....	225

List of Tables

Table 1. RSUs Device Security Class by Service Package	9
Table 2. Control Specifications by Device Security Class RSU	16
Table 3. Adversarial Threat Events	149
Table 4. Non-Adversarial Threat Events	155
Table 5. Physical Object Threat Events	156
Table 6. Vulnerabilities and Predisposing Conditions	157
Table 7. Mapping of RSU Mission Objectives to NIST CSF Subcategories and NIST SP 800-53 Controls	161

List of Figures

Figure 1. Diagram. RSU Context Diagram from NTCIP 1218 v01.38 ⁽⁴⁷⁾	6
Figure 2. Diagram. V2X System	7
Figure 3. Diagram. RSU Mounted on a Mast Arm of a Traffic Signal	8

Chapter 1. Identification

Purpose, Scope, and Applicability

This control set document defines the security and privacy controls necessary to address risks specific to roadside units (RSUs) 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 RSU assets and their associated information flows. As RSU technology evolves to support advanced features, this control set aims to mitigate risks inherent to RSU operations and interfaces, helping to ensure secure and reliable communication with vehicles and infrastructure components.

Designed for use by system owners, managers, integrators, engineers, and manufacturers, this control set offers a structured approach to identifying security requirements for RSUs. The outlined controls, primarily technical in nature, complement broader ITS security measures and include necessary organizational controls from NIST SP 800-53⁽¹⁾ relevant to the design, implementation, and operational support of RSUs. Additionally, these controls help address residual risks from overarching ITS infrastructures that may impact RSUs, helping to protect against unauthorized access, data manipulation, and service disruptions. By referencing the larger security posture of ITS systems, RSU stakeholders can identify gaps and apply controls specific to RSUs to mitigate unaddressed risks.

This proactive approach ensures that critical technical controls essential to RSU security are integrated, whether by manufacturers, infrastructure operators, or organizational stakeholders, to maintain secure, resilient ITS environments. The controls (primarily technical controls) relevant to RSUs 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. 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 RSUs.

The risk mitigation and protection provided by other controls implemented in larger systems, operations, or data centers, or by the infrastructure owner/operators (IOOs) operating ITS, benefit physical objects that are part of these larger systems, centers, or IOOs. Owners, operators, and users of RSUs may examine the security assessment of the larger system to determine which risks might not be mitigated and/or might be passed on to RSUs themselves and then select controls that mitigate those risks. 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 is critical for successfully securing the RSU. Such controls are addressed by the IOO before, during, or after an RSU is delivered and installed.

The scope of this control set focuses primarily on how a typical RSU 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 RSU 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" in 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*.⁽²⁾
- NIST issues new revisions of SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*.⁽¹⁾
- NIST issues new revisions of SP 800-82, *Guide to Industrial Control Systems (ICS) Security*.⁽³⁾
- NIST issues new revisions of The Cybersecurity Framework (CSF).⁽⁴⁾
- Architecture Reference for Cooperative and Intelligent Transportation (ARC-IT)⁽⁵⁾ is significantly revised in areas that affect RSUs.
- 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 NCTIP 1218 v01.38, *Object Definitions for Roadside Units (RSUs)*.⁽⁴⁷⁾
- Connected Transportation Interoperability (CTI) makes significant changes to CTI 4001 v01.01 - Roadside Unit (RSU) Standard Amendment.⁽⁶⁾

Sources

The following are key resources used to create this document and guide the identification of controls needed to mitigate risks to RSUs. Each resource includes a brief context explaining how it influenced or informed the selection of controls.

- ARC-IT version 9.3, for device security classes based on the potential impact to the confidentiality, integrity, and availability of information flows between physical objects and their associated functional objects.⁽⁷⁾
- NIST SP 800-30, Revision 1, for typical threat sources and vulnerabilities that may be relevant or tailored to ITS.⁽²⁾
- NIST SP 800-82, Revision 3, for industrial control system (ICS) 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.⁽⁸⁾
- 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.⁽⁹⁾
- ITS CSF 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⁾

- NCTIP 1218 v01.38, *Object Definitions for Roadside Units (RSUs)*, for overall object definition and industry standards for RSU communication.⁽⁴⁷⁾
- CTI 4001 v01.01, *Roadside Unit (RSU) Standard Amendment*, for current RSU standards.⁽⁶⁾

Relationship between ARC-IT, CSF, 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 CSF 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.⁽⁷⁾ 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 requirements.
- **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 a 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.⁽¹¹⁾

Cybersecurity in ARC-IT⁽¹²⁾ is addressed through the analysis of the confidentiality, integrity, and availability (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.⁽⁷⁾ 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 controls¹) relevant to the RSUs 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 RSUs 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.^(13,14)

¹ The technical controls are typically implemented by systems rather than by people.

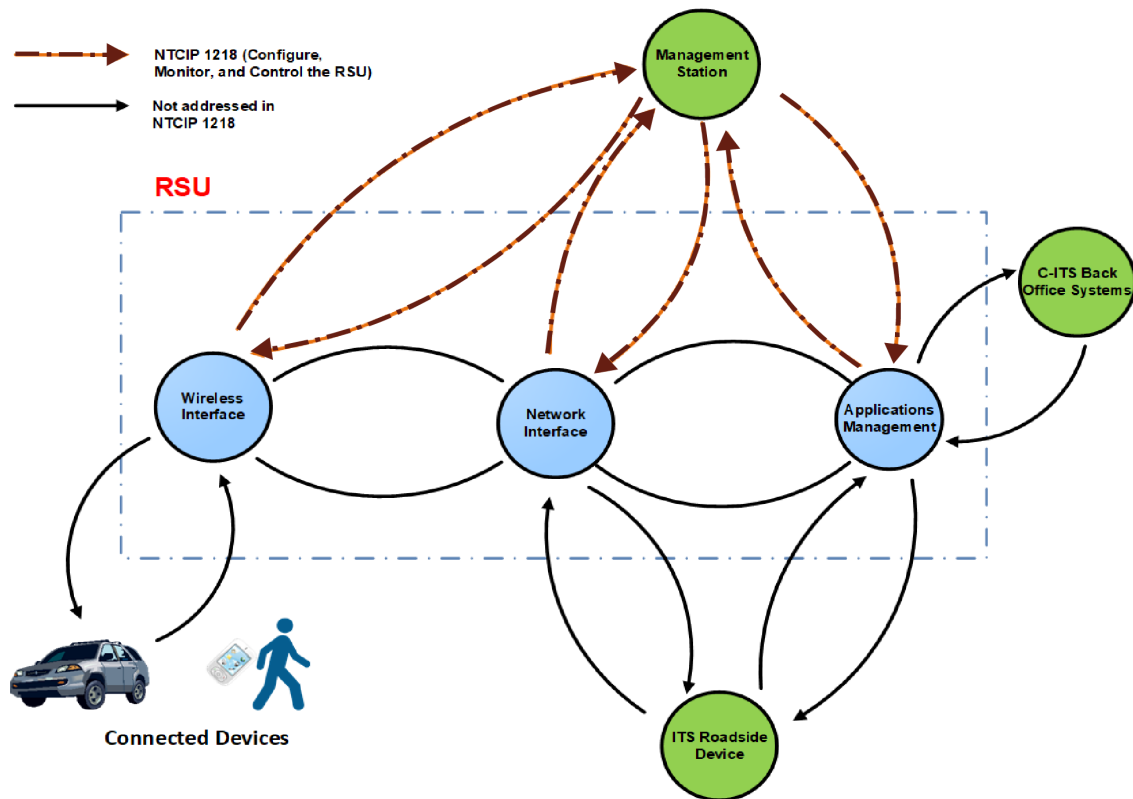
Chapter 2. Physical Object Characteristics

Definition/Description

ARC-IT defines the RSU as a field device that facilitates secure communications with connected devices, other ITS roadside devices, and traffic management systems (TMS). The RSU serves as a key component in vehicle-to-everything communication (V2X) and represents connected vehicle roadside equipment (CVRSE), enabling data exchange among connected vehicles, mobile devices/pedestrians, and infrastructure systems to support ITS operations. By supporting V2X communication through industry-standard protocols such as IEEE 802.11,⁽¹⁵⁾ IEEE 1609.2,⁽¹⁶⁾ SAE J2735™,⁽¹⁷⁾ and SAE J2945™,⁽¹⁸⁾ RSUs enhance road safety, traffic efficiency, and mobility.

This control set ensures the C-I-A of RSU operations within the cooperative-ITS (C-ITS) environment. Security measures focus on protecting wireless, wired, and physical interfaces to prevent unauthorized access and data tampering, maintaining system functionality to ensure resilience against disruptions, and safeguarding data flows to support secure and uninterrupted communication between connected devices, roadside systems, and traffic management centers (TMCs).

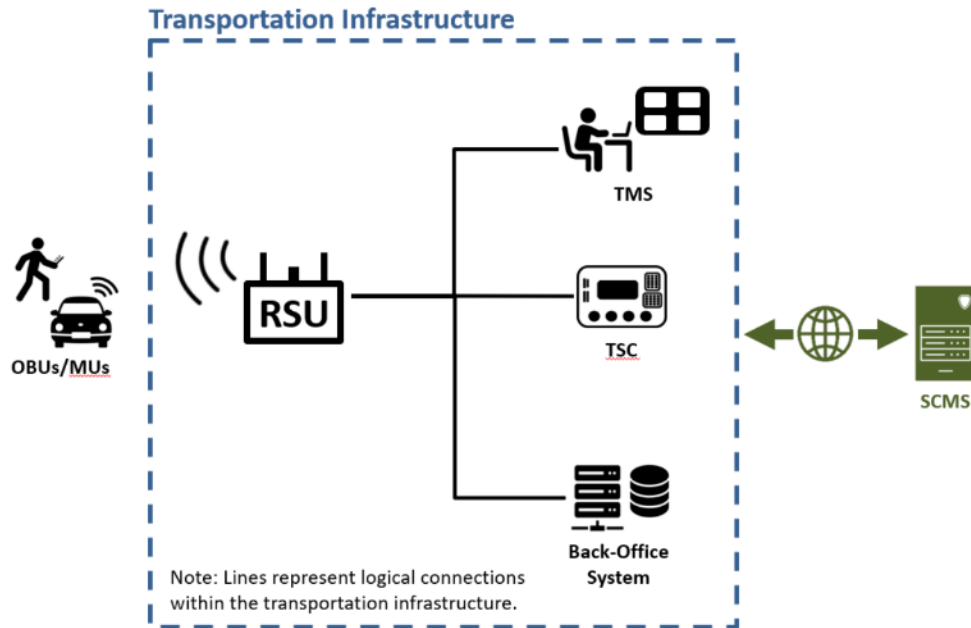
The RSU comprises three primary components, shown in Figure 1. The V2X interface enables wireless communication with vehicles and other connected devices. The network interface facilitates data exchange between vehicles, roadside ITS devices—such as traffic signals, environmental sensors, and dynamic message signs—and central TMSs. The applications management component functions as a computing platform, processing inputs from vehicles, ITS devices, and management systems to deliver transportation services. Collectively, these components support V2X communication, route data between connected systems, and host applications that enhance transportation safety and efficiency.



Source: NTCIP 1218 v01.38, September 2020

Figure 1. Diagram. RSU Context Diagram from NTCIP 1218 v01.38.⁽⁴⁷⁾

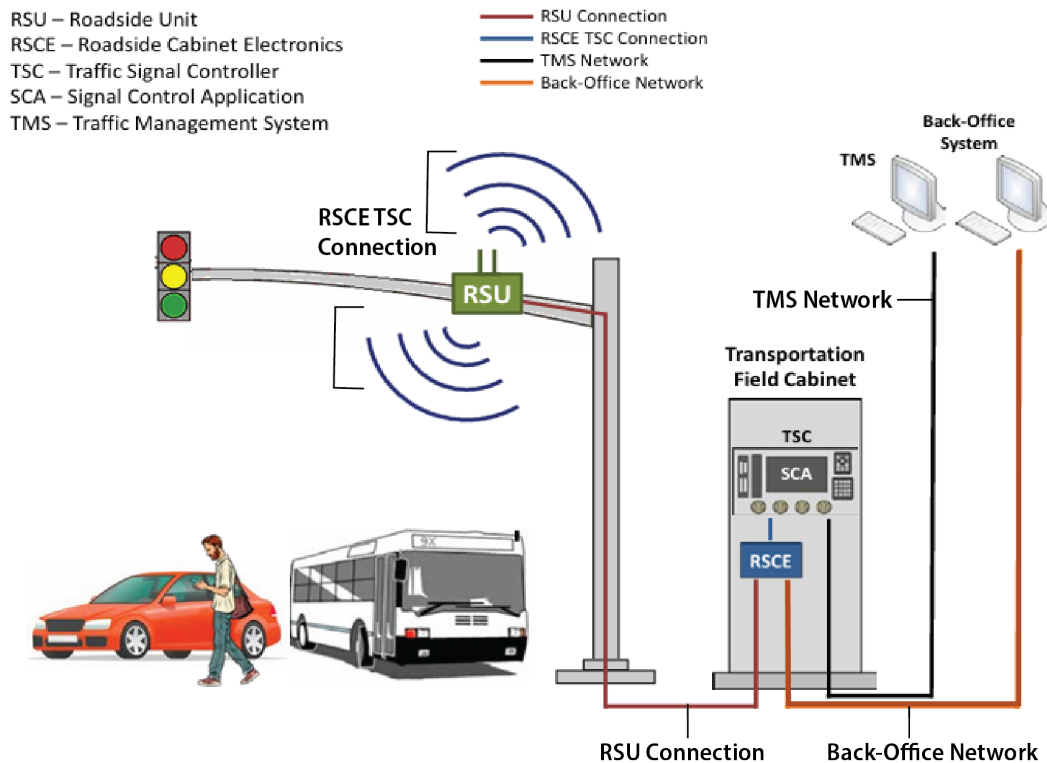
Central to the RSU's secure operation is the security credential management system (SCMS), a public key infrastructure (PKI) system that provides digital certificates to RSUs and onboard units (OBUs) in vehicles. The SCMS ensures the confidentiality, integrity, and availability of V2X communications by issuing short-term certificates, typically valid for one week, which devices use to sign and verify messages, preventing unauthorized access or data tampering. For instance, RSUs validate signal request messages from vehicles for transit signal priority applications and broadcast trusted messages such as collision warnings or traffic updates. This is illustrated by the logical connections between the RSU, TMS, traffic signal controller (TSC), back-office system, and SCMS in Figure 2 CTI 4001 v01.01.⁽⁶⁾



Source: CTI 4001 v01.01 — Amendment 1, September 2022

Figure 2. Diagram. V2X System.

The types and quality of connectivity and interfaces required by RSUs include secure, low-latency wireless communication with connected vehicles and mobile devices, using protocols such as IEEE 802.11⁽¹⁵⁾ and IEEE 1609.x.⁽¹⁶⁾ Network interfaces enable secure data exchanges with ITS roadside devices and TMCs. Local maintenance interfaces, such as Ethernet, or serial connections, may also be used for diagnostics and configuration. An important factor in the V2X system is the RSU's ability to facilitate seamless communication between OBUs/MUs and infrastructure elements, such as TMS or back-office systems. To achieve this, the RSU must be connected to the transportation field cabinet system. This connection is typically established by linking the RSU to the roadside cabinet electronics (RSCE) via Ethernet, which, in turn, is wired to the TSC. Within CTI 4001 v01.01,⁽⁶⁾ it illustrates this connectivity, providing a detailed depiction of the relationships and interfaces between these components shown in Figure 3.



Source: CTI 4001 v01.01 — Amendment 1, September 2022

Figure 3. Diagram. RSU Mounted on a Mast Arm of a Traffic Signal.

The RSU operates in outdoor roadside environments, typically deployed along highways, intersections, or other transportation infrastructure. These environments expose the RSU to varying weather conditions, physical wear, and potential cybersecurity risks, necessitating robust physical and cybersecurity protections. Since the RSU is easily accessible to the public, they are vulnerable to critical physical attacks targeting software, firmware and hardware. Examples of exploitations achieved through physical access to the RSU include inserting malicious drivers and boots off USB devices, gaining root access via the extensible firmware interface (EFI) shell (often enabled by default on new RSU devices), and overwriting firmware through the exposed serial peripheral interface (SPI), among other vulnerabilities. To mitigate these specific RSU vulnerabilities, “Implementation Considerations” in chapter 5 details a collection of security controls that both manufacturers and IOOs should prioritize.

Physical Object Device Security Class by Service Package

Table 1 conveys that the RSU appears in 55 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 physical object may be used within multiple service packages, it is necessary to consider the impact of the physical object 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. RSUs Device Security Class by Service Package.

Service Package	Device Security Class (CVRSE)
CVO06: Freight Signal Priority	2
CVO10: Road Weather Information for Freight Carriers	3
DM01: ITS Data Warehouse	1
MC03: Roadway Automated Treatment	3
MC06: Work Zone Management	2
MC07: Work Zone Safety Monitoring	3
MC09: Infrastructure Monitoring	5
MC10: Asset Tracking	2
MC11: Maintenance and Construction Signal Priority	2
PM01: Parking Space Management	2
PM02: Smart Park and Ride System	2
PS03: Emergency Vehicle Preemption	3
PS07: Incident Scene Safety Monitoring	3
PS09: Transportation Infrastructure Protection	3
PT09: Transit Signal Priority	5
PT10: Intermittent Bus Lanes	3
PT12: Transit Vehicle at Station/Stop Warnings	2
PT15: Transit Stop Request	4
PT16: Route ID for the Visually Impaired	2
ST01: Emissions Monitoring	2

Service Package	Device Security Class (CVRSE)
ST02: Eco-Traffic Signal Timing	2
ST03: Eco-Traffic Metering	2
ST04: Roadside Lighting	2
ST06: HOV/HOT Lane Management	2
ST07: Eco-Lanes Management	3
ST08: Eco-Approach and Departure at Signalized Intersections	3
ST09: Connected Eco-Driving	2
ST10: Low Emissions Zone Management	2
SU01: Connected Vehicle System Monitoring and Management	5
SU04: Map Management	3
SU05: Location and Time	5
TI01: Broadcast Traveler Information	2
TI07: In-Vehicle Signage	2
TM04: Connected Vehicle Traffic Signal System	3
TM14: Advanced Railroad Grade Crossing	5
TM16: Reversible Lane Management	1
TM17: Speed Warning and Enforcement	1
TM19: Roadway Closure Management	3
TM21: Speed Harmonization	2
TM22: Dynamic Lane Management and Shoulder Use	2
TM24: Tunnel Management	2
TM25: Wrong Way Vehicle Detection and Warning	1
VS05: Curve Speed Warning	2

Service Package	Device Security Class
VS06: Stop Sign Gap Assist	5
VS07: Road Weather Motorist Alert and Warning	3
VS08: Queue Warning	2
VS09: Reduced Speed Zone Warning / Lane Closure	2
VS10: Restricted Lane Warnings	2
VS11: Oversize Vehicle Warning	1
VS12: Vulnerable Road User Safety	3
VS13: Intersection Safety Warning and Collision Avoidance	3
VS15: Infrastructure Enhanced Cooperative Adaptive Cruise Control	3
VS17: Management of Electronic Traffic Regulations (METR)	3
WX01: Weather Data Collection	2
WX03: Spot Weather Impact Warning	3

CVO = Commercial Vehicle Operations; CVRSE = connected vehicle roadside equipment; DM = Data Management; MC = Maintenance and Construction; PM = Parking Management; PS = Public Safety; PT = Public Transportation; ST = Sustainable Travel; SU = Support; TI = Traveler Information and Personal Mobility; TM = Traffic Management; VS = Vehicle Safety; WX = Weather.

Assumptions and Characteristics

This control set document is necessary because ITS physical objects have a set of characteristics and assumptions that often differentiates them from other types of technologies (e.g., general enterprise information technology). Those assumptions are listed here and are discussed in the following paragraphs:

- Assumption #1: RSUs operate in the Field environment and are reliably in harsh environmental conditions.
 - RSUs are deployed in exposed environments rather than located in buildings. From a risk management perspective, RSUs are more akin to operational technology (OT) than to information technology. For example, Physical and Environmental (PE) controls (e.g., gates, guards, fire detection and suppression, lighting) associated with a fixed facility may not be implemented for RSUs. However, other PE controls that address physical access (e.g., PE-3(4), Physical Access Control | Lockable Casings) or monitoring the environment (e.g., PE-14, Environmental Controls) are needed. RSUs are assumed to perform consistently under

extreme environmental conditions, including high humidity, extreme temperatures, and severe weather events like flooding and snow. This ensures reliable operation across diverse climates.

- Assumption #2: RSUs are connected to a secure network and support modern communication protocols.
 - RSUs are assumed to connect securely to a network using cellular, wireless fidelity (Wi-Fi), or Ethernet. This connectivity allows reliable data exchange with TMCs and other connected infrastructure (e.g. RSCE, TSC). The control set assumes that RSUs utilize contemporary communication protocols, such as FTP, Simple Network Management Protocol, Wireless Access in Vehicular Environments Short Message Protocol, TCPIP Hypertext Transfer Protocol Secure (HTTPS), and secure V2X protocols (e.g., C-V2X). Legacy RSUs with limited or outdated protocol support fall outside the scope of this control set. RSUs operating in isolated or offline modes may require alternative controls not addressed within this set.
- Assumption #3: RSUs support both persistent and non-persistent data.
 - Some data processed by RSU may be more perishable than persistent in nature. As such, not all the data may require the same protections. For example, non-perishable data is stored and, therefore, may require integrity protection to prevent unauthorized changes. In contrast, perishable data is processed and discarded so quickly that it may not require similar protections. RSU data may be used by physical objects or vehicles and may also be collected, correlated, analyzed, or otherwise processed for human consumption and decisions. Each “phase” of the data’s lifecycle may have unique protection requirements. Also, it is possible the data is collected and used in a way not originally intended or for which RSUs were designed; therefore, additional security protections may be necessary.
- Assumption #4: RSU’s may be designed with antennas mounted away or on the RSU.
 - Some architecture designs have the antennas of the RSU mounted on the mast arm of a traffic light system, while other designs have the antennas integrated directly into the RSU. It is important to address the physical safety of each design differently, considering the unique vulnerabilities associated with each approach. For designs where the antennas are mounted on the mast arm, potential vulnerabilities include increased exposure to environmental factors (e.g., wind, ice, and debris), as well as ease of access for tampering or vandalism due to the antenna’s elevated and potentially less secure placement. Protective measures such as reinforced mounting, weatherproof enclosures, and tamper-proof fasteners may be required. In contrast, designs with antennas integrated directly into the RSU may have a more compact and secure setup, but they could still be vulnerable to physical damage if the RSU is placed in a high-traffic or easily accessible area. Additionally, integration may complicate maintenance or upgrades if the antenna needs replacement or repair.
- Assumption #5: RSUs are expected to support firmware and software updates remotely.
 - RSUs should have mechanisms to securely receive and install firmware and software updates remotely. This includes the use of secure update protocols (e.g., digitally signed firmware, HTTPS) to protect against tampering and ensure the integrity of updates. This also implies that RSUs need reliable network connectivity and sufficient storage capacity for update processes.

Resources for Identifying Threats, Vulnerabilities, and Predisposing Conditions

A broad set of table 3 (adversarial) and table 4 (non-adversarial) threat events that could potentially impact RSU is provided in 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⁽²⁾ that could potentially impact RSU's is provided in table 3 (adversarial) and table 4 (non-adversarial) below. The properties of RSU's may also present unique opportunities to a threat source, specifically addressing how the threat source can manipulate the process of the RSU's to cause damage or achieve other malicious purposes (e.g., exfiltration of data). table 4 provides an overview of potential threat events from NISTSP 800-82⁽³⁾ that are more specific to RSU's. Threat events listed below focus on the RSU's (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 RSU's or its mission/operations, either by compromise of the RSU 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 RSU's can implement a protection measure to mitigate the risk will the threat be considered relevant to the RSU itself and, therefore, controls will be selected in this document to mitigate those risks. In appendix A. The properties of RSU may also present unique opportunities to a threat source, specifically addressing how the threat source can manipulate the process of the RSU in table 5, which provides an overview of potential threat events more specific to the RSU. Table 6 contains any vulnerabilities and predisposing conditions that may impact RSU systems given the uniqueness of the system.

Threat events listed in appendix A focus on the RSUs, not the larger system comprised of various types of physical objects and other components. Various threat events may ultimately impact a RSU or its mission/operations, either by compromise of the RSU 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 RSU can implement a protection measure to mitigate the risk will the threat be considered relevant to the RSU itself and, therefore, controls will be selected in this document to mitigate only those risks. Only if the RSU can implement a protection measure to mitigate the risk will the threat be considered relevant to the RSU 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 Profile, a comprehensive table was developed to map relevant mission objectives for the RSU system to NIST CSF subcategories, as presented in table 7. These mission objectives were defined based on the RSU system's physical and technical attributes, such as its data processing capabilities and wireless communication features. The following mission objectives were chosen for the RSU system: #1: Improve physical safety of the transportation ecosystem, #2: Increase the efficiency of the transportation ecosystem, #3: Collect, manage, use, and disseminate data, #7: Enhance the integration and connectivity of the transportation system through technology, #8: Build privacy protections into ITS operations, #10:

Maintain secure technology (information technology/OT) and communications, 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 RSU system. Using the NIST CSF Informative reference tool, appropriate NIST SP 800-53⁽¹⁾ controls were identified to address the RSU 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 RSU 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. The controls are each assigned symbols indicating specific attributes, as defined below, and are categorized according to the device security classes specified in ARC-IT. Not all device security classes will be assigned to implement more intricate security controls. In such cases, the symbol “NS” indicates non-applicability. The controls and enhancements were selected to secure the RSU system while considering its technical and physical properties. Responsibilities for implementing the controls 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 implementation tailoring guidance.
- “V” indicates this control set document defines a value for an ITS-specific parameter for the control,² 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 best 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 element³ for each control in NIST SP 800-53.⁽¹⁾ Unique implementations are described in the guidance provided in “Detailed Control Specifications” in Chapter 4 of this control set document. The last column of Table 2 below indicates if the control should be implemented by the manufacturer within or for the physical object and by the IOO organization. Allocation of responsibility for the controls may be different than what is implied in the 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.

² 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.

³ The Discussion element was previously called Supplemental Guidance in NIST SP 800-53 Revision 4.

Table 2. Control Specifications by Device Security Class RSU

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	M/I
AC-2(5)	Inactivity Logout	NS	GVRs	GVRs	GVRs	GVRs	M/I
AC-3	Access Enforcement	GR	GR	GR	GR	GR	M/I
AC-3(2)	Dual Authorization	GVR	GVR	GVR	GVR	GVR	I
AC-3(4)	Discretionary Access Control	NS	NS	GR	GR	GR	M/I
AC-4	Information Flow Enforcement	GVRs	GVRs	GVRs	GVRs	GVRs	M/I
AC-4(4)	Flow Control of Encrypted Information	GVS	GVS	GVS	GVS	GVS	M/I
AC-4(14)	Security or Privacy Filter Constraints	G	G	G	G	G	M/I
AC-5	Separation of Duties	GVR	GVR	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	GVR	GVR	GVR	GVR	GVR	I
AC-6(8)	Privilege Levels for Code Execution	GV	GV	GV	GV	GV	M

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-9	Previous Logon Notification	NS	GR	GR	GR	GR	I
AC-10	Concurrent Session Control	GVR	GVR	GVR	GVR	GVR	M/I
AC-11	Device Lock	GVR	GVR	GVR	GVR	GVR	M/I
AC-12	Session Termination	GVR	GVR	GVR	GVR	GVR	M/I
AC-12(1)	User-Initiated Logouts	GV	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	GRS	GRS	GRS	GRS	GRS	M/I
AC-17(1)	Monitoring and Control	GR	GR	GR	GR	GR	M/I
AC-17(2)	Protection of Confidentiality and Integrity Using Encryption	GRS	GRS	GRS	GRS	GRS	M
AC-17(6)	Protection of Mechanism Information	G	G	G	G	G	I
AC-18	Wireless Access	GR	GR	GR	GR	GR	I
AC-18(1)	Wireless Access Authentication and Encryption	NS	GVRs	GVRs	GVRs	GVRs	M/I
AC-18(3)	Wireless Access Disable Wireless Networking	NS	NS	G	G	G	I

ID	Title	Device Security Class					Responsibility (Manufacturer (M); IOO (I))
		1	2	3	4	5	
AC-18(5)	Wireless Access Antennas and Transmission Power Levels	GR	GR	GR	GR	GR	I
AC-20	Use of External Systems	GVRs	GVRs	GVRs	GVRs	GVRs	M/I
AC-20(1)	Limits of Authorized Use						I
AC-20(2)	Portable Storage Devices — Restricted Use	GVS	GVS	GVS	GVS	GVS	M/I
AC-21	Information Sharing	GV	GV	GV	GV	GV	I
AC-24	Access Control Decisions	GV	GV	GV	GV	GV	M/I
AT-3	Role-Based Training	GVR	GVR	GVR	GVR	GVR	M/I
AU-2	Event Logging	GVRs	GVRs	GVRs	GVRs	GVRs	I
AU-3	Content of Audit Records	GS	GS	GS	GS	GS	M/I
AU-4	Audit Log Storage Capacity	GVR	GVR	GVR	GVR	GVR	M/I
AU-4(1)	Transfer to Alternate Storage	NS	NS	GVR	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	NS	GVR	GVR	GVR	GVR	I
AU-6(4)	Central Review and Analysis	NS	G	G	G	G	I
AU-6(6)	Correlation with Physical Monitoring	G	G	G	G	G	M/I

ID	Title	Device Security Class					Responsibility
		1	2	3	4	5	
AU-7	Audit Record Reduction and Report Generation	G	G	G	G	G	M/I
AU-9	Protection of Audit Information	GVR	GVR	GVR	GVR	GVR	M/I
AU-9(2)	Store on Separate Physical Systems or Components	NS	NS	NS	GVR	GVR	M/I
AU-9(3)	Cryptographic Protection	NS	NS	GRS	GRS	GRS	M
AU-11	Audit Record Retention	GV	GV	GV	GV	GV	M/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	GV	GV	GV	GV	GV	I
AU-16	Cross-Organizational Audit Logging	GVS	GVS	GVS	GVS	GVS	M/I
CA-3	Information Exchange	GVR	GVR	GVR	GVR	GVR	I
CA-3(6)	Transfer Authorizations	NS	G	G	G	G	I
CA-3(7)	Transitive Information Exchanges	G	G	G	G	G	I
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	GVR	GVR	GVR	GVR	GVR	I
CA-7(4)	Risk Monitoring	G	G	G	G	G	I

ID	Title	Device Security Class					Responsibility (Manufacturer (M); IOO (I))
		1	2	3	4	5	
CA-7(6)	Automation Support for Monitoring	NS	NS	GV	GV	GV	M/I
CA-8	Penetration Testing	GVRs	GVRs	GVRs	GVRs	GVRs	M/I
CA-9	Internal System Connections	GVR	GVR	GVR	GVR	GVR	M/I
CM-2	Baseline Configuration	GVS	GVS	GVS	GVS	GVS	I
CM-3	Configuration Change Control	GR	GR	GR	GR	GR	M/I
CM-4	Impact Analysis	GR	GR	GR	GR	GR	I
CM-5	Access Restrictions for Change	GR	GR	GR	GR	GR	I
CM-5(4)	Dual Authorization	GV	GV	GV	GV	GV	I
CM-6	Configuration Settings	GV	GV	GV	GV	GV	M/I
CM-7	Least Functionality	GVR	GVR	GVR	GVR	GVR	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
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-9	Configuration Management Plan	GV	GV	GV	GV	GV	I

ID	Title	Device Security Class					Responsibility (Manufacturer (M); IOO (I))
		1	2	3	4	5	
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	GVR	GVR	GVR	GVR	GVR	M/I
CP-9(1)	Testing for Reliability and Integrity	GVR	GVR	GVR	GVR	GVR	M/I
CP-9(8)	Cryptographic Protection	GVS	GVS	GVS	GVS	GVS	M/I
CP-10	System Recovery and Reconstitution	GVR	GVR	GVR	GVR	GVR	I
IA-2	Identification and Authentication	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
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	GRS	GRS	GRS	GRS	GRS	M/I
IA-5(14)	Managing Content of PKI Trust Stores	GS	GS	GS	GS	GS	M/I
IA-7	Cryptographic Module Authentication	GRS	GRS	GRS	GRS	GRS	M/I

ID	Title	Device Security Class					Responsibility (Manufacturer (M); IOO (I))
		1	2	3	4	5	
IA-8	Identification and Authentication (Non-Organizational Users)	GR	GR	GR	GR	GR	M
IA-9	Service Identification and Authentication	GRS	GRS	GRS	GRS	GRS	M/I
IA-11	Re-authentication	GV	GV	GV	GV	GV	M/I
IR-2	Incident Response Training	NS	NS	GV	GV	GV	I
IR-3	Incident Response Testing	NS	NS	GV	GV	GV	I
IR-4	Incident Handling	NS	NS	GR	GR	GR	I
MA-2	Controlled Maintenance	GV	GV	GV	GV	GV	I
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

ID	Title	Device Security Class					Responsibility
		1	2	3	4	5	
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	GV	GV	GV	GV	GV	M/I
PE-6	Monitoring Physical Access	GV	GV	GV	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
PE-18	Location of System Components	G	G	G	G	G	I
PE-21	Electromagnetic Pulse Protection	GV	GV	GV	GV	GV	M/I
PL-2	System Security and Privacy Plans	GVR	GVR	GVR	GVR	GVR	M/I
PL-7	Concept of Operations	GVR	GVR	GVR	GVR	GVR	I
PM-5	System Inventory	GV	GV	GV	GV	GV	M/I
RA-3	Risk Assessment	GVS	GVS	GVS	GVS	GVS	M/I
RA-3(1)	Supply Chain Risk Assessment	GVS	GVS	GVS	GVS	GVS	M/I
RA-5	Vulnerability Scanning	GVR	GVR	GVR	GVR	GVR	M/I
RA-5(3)	Vulnerability Scanning Breadth and Depth of Coverage	G	G	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

ID	Title	Device Security Class					Responsibility (Manufacturer (M); IOO (I))
		1	2	3	4	5	
SA-4(2)	Design and Implementation Information for Controls	GVR	GVR	GVR	GVR	GVR	M/I
SA-4(5)	System, Component, and Service Configurations	GV	GV	GV	GV	GV	M/I
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
SA-10(1)	Software and Firmware Integrity Verification	GR	GR	GR	GR	GR	M
SA-10(3)	Hardware Integrity Verification	G	G	G	G	G	M
SA-11	Developer Security Testing and Evaluation	GVR	GVR	GVR	GVR	GVR	M/I
SA-11(2)	Threat Modeling and Vulnerability Analysis	NS	NS	GV	GV	GV	M
SA-11(6)	Attack Surface Reviews	NS	NS	G	G	G	M

ID	Title	Device Security Class					Responsibility (Manufacturer (M); IOO (I))
		1	2	3	4	5	
SA-17	Developer Security and Privacy Architecture and Design	G	G	G	G	G	M
SA-22	Unsupported System Components	GVR	GVR	GVR	GVR	GVR	M/I
SC-2	Separation of System and User Functionality	GR	GR	GR	GR	GR	M
SC-2(1)	Separation of System and User Functionality Interfaces for Non-Privileged Users	G	G	G	G	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	G	G	G	G	G	M
SC-3(3)	Security Function Isolation Minimize Non-Security Functionality						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	G	G	G	G	G	M

ID	Title	Device Security Class					Responsibility (Manufacturer (M); IOO (I))
		1	2	3	4	5	
SC-5(3)	Denial-of-Service Protection Detection and Monitoring	NS	NS	GV	GV	GV	M/I
SC-6	Resource Availability	NS	NS	GV	GV	GV	M
SC-7	Boundary Protection	GVR	GVR	GVR	GVR	GVR	M
SC-7(3)	Boundary Protection Access Points	GR	GR	GR	GR	GR	M/I
SC-7(5)	Boundary Protection Deny by Default — Allow by Exception	GVR	GVR	GVR	GVR	GVR	M
SC-7(7)	Boundary Protection Split Tunneling for Remote Devices	GV	GV	GV	GV	GV	M/I
SC-7(14)	Boundary Protection Protect Against Unauthorized Physical Connections	GVS	GVS	GVS	GVS	GVS	M/I
SC-7(16)	Boundary Protection Prevent Discovery of System Components	G	G	G	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-Organizationally Configured Hosts	GV	GV	GV	GV	GV	M/I

ID	Title	Device Security Class					Responsibility (Manufacturer (M); IOO (I))
		1	2	3	4	5	
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-8(2)	Transmission Confidentiality and Integrity Pre- and Post-Transmission Handling	GVS	GVS	GVS	GVS	GVS	M
SC-11	Trusted Path	GV	GV	GV	GV	GV	M
SC-12	Cryptographic Key Establishment and Management	GVS	GVS	GVS	GVS	GVS	M/I
SC-12(3)	Cryptographic Key Establishment and Management Asymmetric Keys	GVS	GVS	GVS	GVS	GVS	M/I
SC-13	Cryptographic Protection	GVRS	GVRS	GVRS	GVRS	GVRS	M
SC-17	Public Key Infrastructure Certificates	GVS	GVS	GVS	GVS	GVS	M/I
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	GVS	GVS	GVS	GVS	GVS	M
SC-28(3)	Protection of Information at Rest Cryptographic Keys	GVS	GVS	GVS	GVS	GVS	M
SC-32	System Partitioning	GV	GV	GV	GV	GV	M/I
SC-34	Non-Modifiable Executable Programs	GV	GV	GV	GV	GV	M
SC-35	External Malicious Code Identification	G	G	G	G	G	M
SC-39	Process Isolation	GR	GR	GR	GR	GR	M
SC-39(1)	Hardware Separation	G	G	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	GV	GV	GV	GV	GV	M/I
SI-2	Flaw Remediation	GVR	GVR	GVR	GVR	GVR	M/I
SI-2(4)	Flaw Remediation Automated Patch Management Tools	GV	GV	GV	GV	GV	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	System Monitoring	GVRs	GVRs	GVRs	GVRs	GVRs	M/I

ID	Title	Device Security Class					Responsibility (Manufacturer (M); IOO (I))
		1	2	3	4	5	
SI-4(2)	System Monitoring Automated Tools and Mechanisms for Real-Time Analysis	NS	NS	R	R	R	M
SI-4(4)	System Monitoring Inbound and Outbound Communications Traffic	GVR	GVR	GVR	GVR	GVR	M/I
SI-4(7)	System Monitoring Automated Response to Suspicious Events	NS	NS	GV	GV	GV	M/I
SI-4(15)	System Monitoring Wireless to Wireline Communication	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	GVR	GVR	GVR	GVR	GVR	M/I
SI-7(6)	Software, Firmware, and Information Integrity Cryptographic Protection	NS					M
SI-7(9)	Software, Firmware, and Information Integrity Verify Boot Process	VR	VR	VR	VR	VR	M

ID	Title	Device Security Class					Responsibility (Manufacturer (M); IOO (I))
		1	2	3	4	5	
SI-7(10)	Software, Firmware, and Information Integrity Protection of Boot Firmware	GVRs	GVRs	GVRs	GVRs	GVRs	M/I
SI-7(12)	Software, Firmware, and Information Integrity Integrity Verification	V	V	V	V	V	M/I
SI-10	Information Input Validation	GVR	GVR	GVR	GVR	GVR	M
SI-16	Memory Protection	GVR	GVR	GVR	GVR	GVR	M/I
SI-17	Fail-Safe Procedures	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
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	G	G	G	G	G	M/I
SR-10	Inspection of Systems or Components	G	G	G	G	G	M/I
SR-12	Component Disposal	G	G	G	G	G	I

Chapter 4. Detailed Control Specifications

This chapter provides details on the controls specified in “Summary of Control Specifications” in chapter 3. For each control, one or more elements may be provided, as 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 RSU (not every possible instantiation) consistent with the assumptions for this control set in “Assumptions and Characteristics” in chapter 2. Where appropriate, the threat sources, vulnerabilities, and/or predisposing conditions in tables 3–6 in appendix A 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 RSU. 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 topic 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 RSU 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, “2nd PV” 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, NIST SP 800-82,⁽³⁾ or ARC-IT) 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 RSU implementation are listed, as not every technique is feasible or possible against a typical RSU. 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 “OT Discussion” for some controls in its overlay for OT. Those discussions are included if relevant to the RSU, but wording may be adapted to the unique features or functions of the RSU.
 - The ARC-IT Mechanisms are requirements-like statements that could be conveyed to a manufacturer/vendor for RSU design and implementation.
 - Standards: This element lists standards relevant to the RSU that prescribe capabilities or cybersecurity requirements.

AC Family – Access Control

AC-1, (Access Control) 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.

For RSUs, access control governance extends beyond administrative access to the device. RSUs participate in a cryptographic trust domain and enforce application-level permissions (e.g., PSIDs and SSPs). Establishing, maintaining, and disseminating access control policies and procedures is required to manage:

- Administrative access to RSUs (local and remote)
- Certificate provisioning and lifecycle management
- Authorization to broadcast specific V2X applications
- Enforcement of PSID/SSP permissions

Guidance: The IOO develops, publishes, and maintains documented access control policies and procedures that define roles and responsibilities for administrative access to RSUs, certificate provisioning and renewal, PSID and SSP authorization management, OpOrgID governance where applicable, and vendor or integrator access to RSU systems.

These policies establish expectations for role-based access control to RSU management interfaces and least-privilege access to configuration settings, firmware management functions, and certificate storage mechanisms. They address separation of duties between operational, security, and vendor personnel and define processes for revoking or modifying access privileges when roles change or personnel transitions occur.

Because RSUs are distributed, field-deployed devices, access control policies account for remote access over public or managed networks, physical access to roadside cabinets, third-party maintenance or contracted support activities, and participation in multi-jurisdictional V2X trust environments where applicable.

Parameter Value(s):

paragraph a. "CISO, Security Administrators, PKI/SCMS Administrators, Domain Administrators, Traffic Operations Managers, and other designated roles with RSU governance responsibilities."

paragraph a.1. "System-level and V2X application-level."

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

paragraph c.1. #2 "device or vendor onboarding, security incidents or suspected misbehavior, intrusion detections, changes to the RSU system configuration, changes to the RSU control set, or changes to certificate issuance, PSID assignments, SSP definitions, or OpOrgID governance."

paragraph c.2. #1 at least annually"

paragraph c.2. #2 "device or vendor onboarding, security incidents or suspected misbehavior, intrusion detections, changes to the RSU system configuration, changes to the RSU control set, or changes in SCMS trust relationships (e.g., new CTL installed)."

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.

Improperly managed accounts directly affect the cybersecurity posture of RSUs and any connected ITS infrastructure. Because RSUs are typically accessed only by operational users such as installers, maintainers, and administrators, who often require elevated privileges, account management becomes an important control for protecting configuration integrity, certificate handling, and firmware management functions.

Guidance: This is primarily an organizational control implemented by the Infrastructure Owner/Operator (IOO), not the manufacturer. The IOO establishes and manages account creation, modification, monitoring, and removal processes for all personnel who access RSUs.

Account management practices define eligibility criteria for account issuance, required approvals, access levels, and lifecycle management processes. Access levels are aligned with operational roles and may include distinctions such as read-only access, full administrative access, firmware update permissions, certificate management access, or serial/console-level access. Account privileges reflect least-privilege principles and are tied to job title or operational role.

Because RSUs are field-deployed devices with elevated operational impact, timely account review and adjustment is critical. Changes in employment status, operational assignment, or trust relationships are reflected in account modifications without delay. The IOO reviews active accounts on a defined recurring basis to validate continued need-to-know justification and appropriate privilege alignment.

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, firmware updating permissions, serial terminal access, certificate management permissions)."

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:

ATT&CK for ICS Mitigations / Techniques:

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

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

ARC-IT Mechanisms:

- Often attackers will leverage compromised user accounts when they know they will not be authenticated. Consider restricting access to some aspects of corporate accounts or prevent users from logging in while they are on vacation, in off hours or over holidays.
- Having the capability to restrict user access to various systems when they are being serviced or updated can also be a handy feature to ensure information system data integrity is preserved during system maintenance.
- The organization will employ a wide range of heuristics to monitor and report on user activity. Common heuristics to look for include source location, source device identifiers, time of day heuristics, typical usage behaviors, and abnormalities in file access or atypical download sizes.

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

Responsible Party (M/I): M/I

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

Guidance: This control addresses the need to disable accounts when predefined conditions are met, including termination, transfer, inactivity, or security concerns.

The IOO defines account disablement timeframes in policy and enforces them through centralized account management systems and through device-level mechanisms on the RSU. The RSU supports administrative and operator-level functionality to disable or lock accounts locally when necessary.

Where RSUs operate in disconnected or semi-connected environments, account disablement capabilities remain available at the device level to prevent continued access in the event of network disruption.

Parameter Value(s):

- #1 “Not to exceed 72 hours”
- paragraph (d) “90 days”

Risk References and Resources:

NIST SP 800-82: When the ITS (e.g., field devices) cannot support

Temporary or emergency accounts, this enhancement does not apply. Example compensating controls include employing nonautomated mechanisms or procedures.

Standards:

NIST SP 800-82 Guide to Operational Technology (OT) Security

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

Responsible Party (M/I): M/I

Justification to Select: Non-Adversarial threat event “Incorrect privilege settings” in table 4.

Guidance: Account management actions generate audit records to support monitoring and forensic analysis. While centralized identity systems at the TMC or enterprise layer typically perform account provisioning and oversight, the RSU supports authentication logging. Most operating systems provide native logging capabilities for account creation and modification events. The IOO ensures that account-related activities affecting RSUs are captured, retained, and periodically reviewed. Automated audit actions help detect incorrect privilege settings, unauthorized account creation, or abnormal access patterns.

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

Responsible Party (M/I): M/I

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

Guidance: The IOO defines inactivity conditions or timeframes under which users manually log out of RSU interfaces. This control is policy-based and depends on user behavior rather than automatic enforcement mechanisms, which are addressed separately under AC-11 (Device Lock).

The RSU provides a visible and accessible logout capability across all management interfaces, including local console, web-based interfaces, and management APIs, allowing the IOO’s inactivity policies to be implemented effectively.

Because RSUs are often accessed in field environments, inactivity expectations consider scenarios where personnel may leave cabinets open or terminals unattended during maintenance activities.

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: 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: NIST SP 800-82 Guide to Operational Technology (OT) Security⁽³⁾

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: Access enforcement mechanisms are implemented at the RSU to ensure that only authenticated and authorized users, systems, or services obtain access consistent with their assigned role and privileges. Enforcement applies to local console access, web or API-based management interfaces, remote maintenance connections, and any service interfaces exposed to upstream systems.

Access enforcement is not limited to user login authentication. It includes enforcement of role-based privileges, restriction of administrative functions, limitation of firmware and configuration modification capabilities, and protection of certificate-related operations. Where RSUs support application configuration functions that influence PSID or SSP behavior, access enforcement also extends to those authorization controls.

Risk References and Resources:

NIST SP 800-82:⁽³⁾ The organization ensures access enforcement mechanisms do not adversely impact the operational performance of the ITS. Example compensating controls include encapsulation. 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 (see the PE family of controls) may serve as a compensating control for logical access control; however, it may not provide sufficient granularity in situations where 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: For high-impact administrative functions, dual authorization adds an additional layer of protection against unauthorized or accidental changes. The IOO identifies functions that warrant enhanced protection and defines when two distinct authorized individuals must participate in approval or execution.

In the RSU context, dual authorization may apply to remote access from the TMC, firmware updates, changes to communication protocols or security keys, modification of configuration parameters affecting broadcast behavior, or other actions that materially affect system integrity or trust relationships.

Dual authorization is implemented through procedural controls, system workflow mechanisms, or centralized management platforms, depending on the deployment architecture. The objective is to reduce the likelihood that a single compromised account or insider action can result in unauthorized system modification.

Parameter Value(s):

“remote access from the TMC, firmware updates, changes to communication protocols or security keys, configuration modifications, etc.”

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.

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: Discretionary access control mechanisms allow the IOO to define and manage user privileges in alignment with organizational policy and operational roles. The IOO establishes access control policies and associated training requirements to ensure personnel understand permitted actions and limitations.

The RSU provides the technical capability to support flexible access control policies, including differentiated privilege levels, configurable permission sets, and centralized management where integrated with TMC or enterprise identity systems. This enables the IOO to modify access parameters as operational needs evolve without requiring device replacement. Physical access controls may supplement discretionary logical controls but do not provide sufficient granularity when users require differentiated administrative or maintenance privileges.

Risk References and Resources:

NIST SP 800-82: 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-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).

RSUs participate in multiple, distinct communication domains, including V2X broadcast interfaces, GNSS inputs, management networks, and back-office backhaul connections. Without defined and enforced information flow boundaries, sensitive management traffic, credential exchanges, or operational data could be exposed or misdirected.

Guidance: The Infrastructure Owner/Operator (IOO) defines information flow control policies to ensure that communications between RSUs, V2X radios, GNSS receivers, field devices, and back-office systems occur only through authorized and explicitly defined interfaces. These flows align with ARC-IT service packages and the intended physical and logical data flows for connected vehicle environments.

Information flow enforcement distinguishes between broadcast V2X traffic and routable management or backhaul traffic. V2X radio transmissions are intentionally broadcast and protected through certificate-based signing and verification mechanisms, while management and configuration traffic is restricted to authorized endpoints over defined network paths.

The manufacturer or vendor implements these policies through logical and physical segmentation of RSU interfaces, including separation of C-V2X or DSRC radio interfaces, Ethernet management ports, cellular backhaul links, and serial or maintenance connections. Segmentation mechanisms may include firewall rules, VLAN separation, access control lists, interface binding, or roadside gateway controls.

Information flow enforcement restricts traffic to organization-defined message types, protocols, ports, and destinations. Outbound connections from the RSU to unmanaged or public networks are

restricted unless explicitly authorized for operational purposes. Where feasible, allow-listing mechanisms are used to define approved endpoints and services.

Parameter Value(s):

“Information-flow controls that restrict V2X and GNSS data exchanges to authorized back-office and roadside networks consistent with ARC-IT service package data flows, prohibit unauthorized outbound connections from the RSU to unmanaged or public networks, and enforce allow-listing of approved message types, ports, and endpoints.”

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, T0885, T0868, T0842

Standards: NIST SP 800-82 Guide to Operational Technology (OT) Security, IEEE Std. 1609.2-2023⁽⁵¹⁾ Security Services for Applications and Management Messages, ARC-IT Architecture Reference for Cooperative and Intelligent Transportation Systems

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: Encrypted information flows are governed by policy to maintain confidentiality while preserving the ability to enforce network security requirements. In RSU environments, encrypted sessions may include TLS-protected management traffic, secure certificate provisioning exchanges, or encrypted backhaul communications.

The IOO defines which encrypted sessions are permitted and identifies trusted endpoints such as TMC systems, SCMS Managers, or authorized service platforms. RSUs and roadside gateways enforce these policies by restricting encrypted sessions to authorized destinations and terminating sessions that do not conform to approved protocols, cipher suites, or endpoint definitions.

Parameter Value(s):

- #1 "Security policy filters and, where applicable, TLS session metadata inspection at the roadside gateway."
- #2 "Termination of encrypted sessions that do not conform to organization-defined authorized protocols, cipher suites, or endpoints."

Standards: NIST SP-800-82⁽³⁾, IEEE Std. 1609.2

AC-4(14), Information Flow Enforcement | Security or Privacy Filter Constraints

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: RSUs accept and transmit structured data from multiple sources, including OBUs, GNSS receivers, roadside devices, and back-office systems. Security and privacy filter constraints ensure that only properly formatted and authorized data is processed by the RSU.

The IOO defines acceptable data formats, message schemas, field lengths, encoding rules, and file size limits where applicable. Input validation mechanisms at the RSU or roadside gateway enforce these constraints so that malformed messages, unexpected payloads, or unauthorized command structures cannot influence device behavior.

For broadcast V2X messages, validation includes certificate verification and message structure checks consistent with IEEE 1609.2 security services. For routable or management traffic, protocol validation and encrypted communication mechanisms protect against interception, manipulation, or injection of unauthorized content.

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.

RSUs support operational control functions, firmware management, and in some deployments, certificate or security configuration activities. When these responsibilities are concentrated in a single individual or role, the risk of unauthorized changes, accidental misconfiguration, or undetected misuse increases.

Guidance: Separation of duties reduces the likelihood that a single user can both introduce and conceal unauthorized changes to the RSU. The IOO defines role boundaries that distinguish between operational control of the device, system configuration, firmware or software updates, and security administration activities such as account or certificate management.

The manufacturer provides role-based access capabilities within the RSU that allow these responsibilities to be separated at the technical level. This includes differentiated privilege levels and the ability to restrict sensitive functions such as firmware installation, modification of communication parameters, or changes to security settings to authorized roles.

Parameter Value(s)

"system operators who manage V2X communications, engineers who update firmware, and auditors who review data exchanges"

Risk References and Resources:

NIST SP 800-82:⁽³⁾ Example compensating controls include providing increased personnel security and auditing. The organization carefully considers the appropriateness of a single individual performing multiple critical roles.

AC-6, Least Privilege

Responsible Party (M/I): I

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

Improper privilege assignment increases the likelihood of misconfiguration, unauthorized changes, or accidental disruption of RSU operations. Because RSUs often support elevated administrative capabilities and may participate in certificate-based trust ecosystems, over-privileged accounts create unnecessary risk.

Guidance: The Infrastructure Owner/Operator (IOO) applies the principle of least privilege so that users, roles, and connected systems receive only the access necessary to perform defined operational tasks. Privileges are aligned with job title or operational role and are limited to specific functions such as configuration updates, log retrieval, firmware management, or certificate administration.

Operational personnel accessing the RSU from a back-office or management network are restricted to task-specific capabilities. For example, technicians may update configurations or retrieve logs, while administrative roles manage user accounts, security settings, or system updates. Privilege assignments are reviewed periodically to ensure continued alignment with operational responsibilities.

Least privilege principles extend beyond user accounts to service accounts, APIs, and remote management interfaces. Overlapping privileges are minimized to reduce the risk of privilege escalation or misuse.

Where strict separation of roles is not feasible, compensating controls such as enhanced auditing or supervisory review support accountability.

Risk References and Resources:

NIST SP 800-82:⁽³⁾ 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:

- M0927/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: Access to security-relevant functions and information on the RSU is limited to explicitly authorized roles. The IOO defines which roles may access security functions and establishes procedures governing that access. The manufacturer provides the technical mechanisms within the RSU to enforce role-based restrictions.

Security-relevant functions include activities such as device commissioning, diagnostics, firmware validation, secure boot verification, network parameter configuration, certificate handling, and

management of audit logs. Access to these functions is limited according to operational role and necessity.

Local Administrators, Field Technicians, Remote Administrators, and Vendors may each be assigned distinct privilege sets. For example, field personnel may physically access the console for commissioning or diagnostics, verify firmware and secure boot status, configure radio or IP parameters, and load signed firmware images without performing key generation. Remote administrators may manage certificates, keys, and enrollment processes where applicable, configure cryptographic parameters, and review system and security event logs. Vendors may access firmware version information and perform signature verification activities but are restricted from broader administrative control unless explicitly authorized.

Parameter Value(s):

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

paragraph a. "physically access the console for device commissioning and diagnostics, perform firmware verification and secure boot status check, configure IP addressing and radio parameters, and load signed firmware images (no key generation)

paragraph b. "(for Local Administrators, Field Technicians, and Remote Administrators) firmware version, local configuration logs, audit logs, device certificates, and network configuration data; (for Remote Administrators) remote management of certificates, keys, and SCMS enrollment, Configuration of network interfaces and cryptographic parameters, and Management of system and security event logs; (for Vendors) firmware signature verification and security relevant information, and firmware version"

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: Network access to privileged commands on the RSU is restricted to clearly defined operational scenarios. Commands that can alter the RSU's operational state, security configuration, firmware status, or cryptographic integrity are not broadly accessible over network interfaces.

Remote execution of privileged functions is limited to situations where physical or local access is infeasible or would negatively affect system availability or roadway safety. These conditions are documented and aligned with operational need.

Network paths that allow privileged command execution are controlled through access control lists, authentication mechanisms, and segmentation controls. Logging and monitoring of privileged network-based commands supports oversight.

Parameter Value(s):

#1 "commands or functions that can alter the RSU's operational state, security configuration, or cryptographic integrity"

#2 "specific operational needs where physical or 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., RSUs) 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): M

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

Guidance: RSU software components execute only with the privileges necessary for their intended function. This applies to operating system services, middleware, communication stacks, and application-level processes.

Manufacturers design RSU platforms so that each process operates under a dedicated service or system account with limited access rights. Code modules do not escalate to administrative or root privileges except through explicitly authorized and auditable mechanisms such as signed firmware updates or secure boot processes.

Development and integration toolchains reinforce least privilege principles through sandboxing, container isolation, SELinux or similar policy enforcement, capability bounding, or equivalent runtime controls. Execution as root or administrator is restricted to approved maintenance or firmware update utilities that are digitally signed and verified.

Parameter Value(s):

"RSU operating-system services, middleware, and application modules shall execute only with the privileges of their assigned service or user context; execution as root or administrator is prohibited except for digitally signed and organization-approved maintenance or firmware-update utilities."

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.

Guidance: Privileged functions on the RSU are identified and documented, either by the IOO or in coordination with the manufacturer. These functions typically include firmware installation, modification of communication or cryptographic parameters, certificate handling, user account management, and changes to security logging settings.

The manufacturer implements technical controls within the RSU to prevent non-privileged users from executing these functions. The IOO aligns these restrictions with organizational policy and operational roles.

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).

RSUs expose local and, in many deployments, remote administrative interfaces. Without controls limiting unsuccessful authentication attempts, these interfaces may be susceptible to brute force or credential guessing attacks, particularly where remote access traverses cellular or public network segments.

Guidance: The Infrastructure Owner/Operator (IOO) defines thresholds for consecutive invalid logon attempts and the timeframe within which those attempts are evaluated. The IOO also defines the automated response that occurs when thresholds are exceeded.

The manufacturer implements mechanisms within the RSU or roadside processing application to track unsuccessful authentication attempts and enforce the defined response. This capability supports both centrally managed deployments and disconnected or degraded modes of operation where the RSU cannot rely on real-time coordination with a centralized identity system.

Automated responses may include temporary lockout, delayed authentication prompts, logging of events, or notification to security personnel. Controls are implemented in a manner that balances protection against brute force activity with operational availability requirements, particularly where field access may be required for maintenance or incident response.

Parameter Value(s):

paragraph a. 1st PV: “5”; 2nd PV: “15 minutes”

paragraph b. “Delay next logon prompt for 3 minutes”

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-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: Previous logon notification enhances user awareness by displaying information about recent authentication activity, including the date, time, and source of the last successful and unsuccessful logon attempts.

The manufacturer provides the capability notify about prior logon information to authenticated users upon login. This notification supports early detection of unauthorized access attempts.

The IOO integrates this capability into technician cybersecurity training, including procedures for reporting suspicious access patterns to the appropriate security or IT personnel. Awareness and reporting reinforce detection capabilities, particularly in field deployments where centralized monitoring may not immediately identify anomalous login behavior.

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: Limiting concurrent sessions reduces the risk of session abuse, credential sharing, or unintended overlapping administrative actions.

The IOO defines maximum concurrent session thresholds by account type based on operational role and responsibility. The manufacturer implements enforcement within the RSU control software so that limits apply even when the RSU is operating in a disconnected mode without centralized coordination.

Parameter Value(s):

#1 "Local Device Administrator, Vendor (disabled by default), Maintenance/Backup Admin, Operator/Technician, and Remote Manager"

#2 "one concurrent session for Local Device Administrator, Vendor, and Maintenance/Backup Admin; two concurrent sessions for Operator/Technician and Remote Manager"

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. The RSU must be capable of automatically locking after a designated period of inactivity to protect against malicious activity. Without a device locking capability, an attacker could take control of the RSU when an operational user logs in but leaves the system accessible when no longer using the RSU.

Guidance: RSUs deployed in roadside cabinets or maintenance environments may be accessed through local consoles or connected devices. Device locking mechanisms prevent unauthorized use when an authenticated user leaves the interface unattended.

The IOO defines inactivity thresholds for manual locking. The manufacturer provides the capability for automatic device lock after a defined period of inactivity and supports user-initiated locking.

When a session is locked by one user, the RSU permits other authorized users to authenticate independently without disrupting normal device operations. Locking affects the session interface, not the RSU's operational functions.

Parameter Value(s):

paragraph a. "initiating a device lock after no more than 5 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 "Conduct externally based session hijacking" in table 3, Conduct an Attack (i.e., direct/coordinate attack tools or activities).

Guidance: Session termination policies define when and how authenticated sessions are ended to prevent hijacking or prolonged exposure.

The IOO defines trigger conditions for terminating sessions, including inactivity, logout, detection of a security event, time-of-day restrictions, or operational boundaries such as shift changes.

The manufacturer implements technical capabilities within the RSU to enforce these conditions for local and remote sessions. Session termination applies to maintenance laptops, remote management interfaces, and back-office connections.

Parameter Value(s):

“15 minutes of inactivity, user logout or security incident detection, end of scheduled shift, or time-of-day limit for remote access.”

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.

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: All authenticated RSU interfaces include a logout capability that allows users to terminate their session voluntarily. This applies to local console interfaces, web-based configuration portals, SSH sessions, and any authenticated API.

Logout actions immediately invalidate active session identifiers, authentication tokens, or cryptographic session keys associated with that user session. This reduces the likelihood of session hijacking or unauthorized reuse.

Parameter Value(s):

“Provide a user-initiated logout capability for all authenticated RSU interfaces (local console, web UI, SSH) that immediately terminates the session and invalidates any active session tokens or keys.”

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).

RSUs intentionally transmit publicly receivable V2X broadcast messages as part of their safety mission. At the same time, administrative and security-relevant functions require strong identification and authentication controls. Clear definition of which actions are permitted without user authentication prevents unintended exposure of sensitive capabilities.

Guidance: The IOO identifies and documents in the system security plan the specific RSU functions that are intentionally permitted without user identification or authentication. For an RSU, these actions are generally limited to standards-defined V2X broadcast activities that are designed to be openly receivable by compliant ITS stations.

In a connected vehicle environment, broadcast transmission does not require authentication at the network access layer. Message authenticity and integrity, however, are enforced cryptographically in accordance with IEEE 1609.2. Each transmitted message is digitally signed using an application certificate issued under an approved SCMS manager, and receiving systems validate the certificate chain, PSID permissions, and SSP constraints before processing the message.

As a result, while user authentication is not required to receive broadcast V2X safety messages, authentication of message origin is performed at the message layer. Authorization to transmit specific application messages is governed through PSID and SSP validation rather than user login mechanisms.

The manufacturer designs the RSU control software so that broadcast transmission functions are clearly separated from management and control-plane functions. Safety message broadcasts such as SPaT, MAP, TIM, or RSM operate without interactive user authentication, but modification of PSID assignments, changes to SSP configuration, certificate installation or enrollment, CRL updates, radio parameter configuration, firmware updates, and secure boot configuration remain restricted to authenticated and authorized administrative roles.

The IOO documents the rationale for permitting unauthenticated broadcast reception and transmission, referencing transportation safety and interoperability requirements. No management, configuration, cryptographic, or other security-relevant function is exposed without identification and authentication. Permitted unauthenticated actions are confined to those necessary for interoperability under IEEE 1609.x and related standards and do not extend to management interfaces, NTCIP objects, or SCMS interactions.

Parameter Value(s):

“Standards-defined V2X broadcast message transmission and reception functions intended for open radio reception under IEEE 1609.x, excluding any management-plane, certificate lifecycle, PSID/SSP configuration, firmware, secure boot, or cryptographic key management functions.”

AC-16, Security and Privacy Attributes

Responsible Party (M/I): M/I

Justification to Select: Threat “Inadequate organizational ownership of risk assessments” in table 3, Conduct an Attack (i.e., direct/coordinate attack tools or activities).

Guidance: The IOO documents RSU information flows in the system security plan and defines the required security attributes for each flow. For every defined data flow the IOO identifies whether integrity protection, authentication, encryption, retention limits, or access restrictions are required. For RSUs, this typically includes distinguishing between publicly receivable broadcast safety messages, management-plane communications, operational logs, configuration data, and protected cryptographic material. Broadcast V2X messages may be publicly receivable but still require cryptographic integrity and origin authentication in accordance with IEEE 1609.2. In contrast, private keys, enrollment credentials, security configuration data, and management traffic require confidentiality protections, strict access controls, and controlled retention.

Parameter Value(s):

paragraph a. #1 "Information classification; sensitivity level; retention period; access authorization; PII indicator; cryptographic protection level"

paragraph a. #2 "{Public, Internal Use, Controlled}; {Low, Medium, High}; {24 hr, 30 days, 1 year, etc.}; {Operator, Administrator, Vendor, Maintenance}; {Yes, No}; {AES-128, AES-256}.

paragraph c. #1 "Servers, databases, roadside processing applications, and storage systems that process, store, or transmit RSU operational or management data."

paragraph c. #2 "Information classification, access authorization, and cryptographic protection level for each defined RSU system component."

paragraph d. "Classification levels may not exceed 'Controlled'; sensitivity ratings are limited to 'Low or Moderate'; cryptographic protection must meet or exceed AES-128; retention periods must fall within IOO-defined limits for ITS data categories."

paragraph f. #1 "Information classification; sensitivity level; retention period; access authorization; PII indicator; cryptographic protection level"

paragraph f. #2 "Annually or upon system configuration change, introduction of new data types, or modification of data-sharing agreements."

Standards: ISO 27002:2022 Control 5.12 - Classification of Information; ISO 27002:2022 Control 5.13 - Labelling of Information⁽⁴⁴⁾; FIPS 199⁽⁴⁵⁾; FIPS 140-3⁽³⁴⁾

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.

Remote access to RSUs introduces elevated risk because management interfaces may traverse public, cellular, or semi-trusted networks. Improperly secured remote access can result in unauthorized configuration changes, firmware manipulation, or compromise of certificate-related functions.

Guidance: The IOO defines the conditions under which remote access to RSUs is permitted, including authorized roles, authentication requirements, approved access paths, time-of-day or maintenance window constraints, and logging expectations. Remote access is limited to operational or maintenance purposes and is not continuously exposed without documented justification.

The manufacturer provides the capability to enforce these policies using secure, encrypted channels such as mutually authenticated TLS-based VPN tunnels or certificate-based SSH sessions. Where TLS is used for connectivity between ITS stations or backend systems, implementations align with ISO 21177 profiles for secure ITS station communications. Remote sessions use NIST-approved cryptographic algorithms and are implemented within FIPS 140-3 validated cryptographic modules where applicable.

All remote connections are logged, including session establishment and termination events, and are subject to monitoring consistent with AC-17(1). Where direct remote access to the RSU is not feasible or advisable, access may be mediated through a roadside gateway or centralized management system.

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

Standards: FIPS 140-3⁽³⁴⁾, FIPS 197⁽³⁵⁾, NIST SP 800-56A⁽²⁴⁾, NIST SP 800-57⁽²⁹⁾, RFC 8446⁽²⁰⁾, RFC 4253, IEEE Std. 1609.2⁽¹⁶⁾, NIST SP 800-82.

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 defines how remote access to RSUs is monitored, including what events are logged, how logs are reviewed, and what constitutes anomalous or unauthorized behavior. Monitoring applies to all external management connections, whether direct to the RSU or mediated through a roadside gateway or centralized management platform.

The manufacturer enables the RSU to generate audit records for remote session establishment and termination, authentication success and failure events, source identifiers (e.g., IP address or certificate identity), and administrative actions performed during remote sessions where technically feasible. Logging applies to TLS-based tunnels, VPN sessions, SSH connections, and other approved remote access mechanisms.

Logs are made available for centralized collection and correlation at the TMC or enterprise monitoring system. Where continuous automated monitoring is not possible, compensating controls such as time-bound access enablement, manual review procedures, or explicit access activation prior to maintenance activities are implemented.

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: Remote access sessions are protected using modern cryptographic protocols that provide confidentiality, integrity, and mutual authentication. The RSU supports establishment of secure tunnels using TLS 1.3 or equivalent contemporary protocols with certificate-based mutual authentication of both endpoints.

Where remote connectivity occurs between ITS stations or between an RSU and backend ITS infrastructure over IP networks, implementations align with ISO 21177 profiles for secure ITS station communications. Cryptographic algorithms and key exchange mechanisms are consistent with NIST-approved standards and are implemented within FIPS 140-3 validated cryptographic modules where applicable.

Risk References and Resources:

NIST SP 800-82:⁽³⁾ 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., VPNs) 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: RFC 8446⁴

AC-17(6), Remote Access | Protection of Mechanism Information

Responsible Party (M/I): I

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

Guidance: Information related to remote access mechanisms is treated as sensitive configuration data. This includes VPN configuration parameters, TLS profiles, endpoint addresses, certificate trust anchors, access control lists, authentication mappings, and maintenance access procedures.

The IOO defines which elements of remote access mechanism information require protection and restricts access to authorized roles. Storage, transmission, and retention of this information are governed by defined security attributes and cryptographic protection requirements.

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.

Guidance: RSUs typically include multiple wireless interfaces that serve different purposes. Some interfaces support management or backhaul connectivity (e.g., cellular, Wi-Fi) while others support V2X safety communications (e.g., C-V2X) that are intentionally broadcast and publicly receivable. This control focuses on preventing unauthorized access through wireless interfaces that could expose management functions, configuration data, or privileged services.

The IOO determines which wireless interfaces are permitted for RSU management or maintenance and documents the approved use conditions, including who may use them, when they may be enabled, and what monitoring is expected. Wireless interfaces not required for operations are

⁴ Internet Engineering Task Force (IETF) Request for Comment 8446, The Transport Layer Security (TLS) Protocol Version 1.3, August 2018.

disabled to reduce attack surface. Wireless configuration changes are limited to explicitly authorized roles.

This control does not attempt to restrict the public receivability of V2X broadcasts. V2X message integrity and origin authentication are handled through IEEE 1609.2 signing and verification, while management-plane wireless access is controlled through authentication, encryption, segmentation, and monitoring.

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/I

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

Guidance: When wireless interfaces are used for RSU management or maintenance, communications are protected with mutual authentication and encryption appropriate to the interface and deployment. The IOO defines usage conditions and approved endpoints; the manufacturer provides the capability to enforce authenticated and encrypted sessions for wireless management channels.

For cellular backhaul or IP-based wireless management paths, encrypted sessions align with organization-approved profiles and may align with ISO 21177 where the connection is ITS station to ITS station over IP. For Wi-Fi or other local wireless maintenance access, authentication and encryption mechanisms prevent unauthorized association and eavesdropping. Cryptographic algorithms follow NIST-approved requirements and use FIPS 140-3 validated modules where applicable.

Parameter Value(s):

“authorized users and authorized devices/endpoints”

Risk and Resources:

NIST SP 800-82: 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 B⁵

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

Responsible Party (M/I): I

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

Guidance: Wireless interfaces not required for RSU operations or maintenance are disabled (or not provisioned) to reduce exposure, particularly any local wireless administration interfaces.

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

Responsible Party (M/I): I

Justification to Select: Threat event “Obtain information by externally located interception of wireless network traffic” in table 3, Conduct an Attack (i.e., direct/coordinate attack tools or activities). Achieve Results (i.e., cause adverse impacts, obtain information).

Guidance: The IOO manages antenna placement and transmission power for wireless interfaces that support management or maintenance access (e.g., Wi-Fi) so signals do not propagate beyond the intended area more than necessary.

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: RSUs may interface with external systems such as maintenance laptops, engineering workstations, vendor support platforms, portable diagnostic devices, TMC systems, or other roadside equipment. In this context, “external” refers to any system operating outside the defined RSU authorization boundary or under a different management authority.

⁵ National Transportation Communications for ITS Protocol (NTCIP) 9014 v01.20, Infrastructure Standards Security Assessment (ISSA), Aug 2021. This standard is referenced to highlight that there is an existing SNMPv3 standard that provides for the use of authentication and encryption, the subject of this control enhancement. Annex B calls for authentication and encryption for SNMPv3.; therefore, by extension authentication and encryption should be used for wireless access.

The IOO defines conditions under which external systems may connect to or interact with RSUs, including acceptable device types, authentication requirements, approved access paths, and logging expectations. The manufacturer provides configuration capabilities within the RSU to enforce these conditions.

Controls applied to external systems may include certificate-based authentication, validation of firmware or software integrity prior to interaction, enforcement of secure communication channels, and logging of connection attempts and administrative actions. External systems that cannot meet defined trust requirements are restricted from direct interaction with RSU management or security functions.

Personally owned or unmanaged devices are not permitted to connect to RSU management interfaces unless explicitly authorized and documented.

Parameter Value(s):

paragraph a. "Document required controls for each authorized external system type, including authentication method, cryptographic protection requirements, firmware or software integrity validation (where applicable), and logging and monitoring expectations."

paragraph b. "Personally owned or unmanaged devices, including external storage media, are prohibited from connecting to RSUs except where explicitly authorized under documented maintenance procedures."

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 Techniques / Mitigations:

- M0801 / T0868, T0886

Standards: FIPS 140-3⁽³⁴⁾; NIST SP 800-46⁽²⁵⁾

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

Responsible Party (M/I): I

Justification to Select: When external systems are authorized for use, the IOO defines explicit limits on how they may interact with the RSU. This includes restrictions on configuration changes, firmware installation, certificate handling, and access to security-relevant logs or cryptographic material.

Authorized use parameters are documented in the system security plan and aligned with defined roles and operational needs. Use of external systems is treated as a managed risk decision rather than a default allowance.

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

Responsible Party (M/I): M/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 RSU storage devices are a common way to compromise a system.

Guidance: Portable storage devices such as USB media present a high risk of malware introduction, unauthorized firmware modification, or configuration tampering in roadside environments. The IOO develops policy limiting or prohibiting the use of portable storage on RSUs except during authorized maintenance activities performed by trained personnel.

If portable media use is approved, devices are scanned on a trusted system prior to connection, and transfers are limited to approved files consistent with defined configuration baselines. Media may be cryptographically signed, write-protected, or otherwise controlled to prevent unauthorized modification.

The manufacturer supports this control by providing the capability to disable USB mass-storage functionality, restrict file system access, enforce read-only modes, or limit accessible directories and file types. During normal operations, USB mass-storage functionality is disabled unless explicitly enabled for a defined maintenance window.

Parameter Value(s):

“Prohibit the use of portable storage devices on RSUs except during authorized maintenance windows. Limit use to organization-approved, malware-scanned, and cryptographically validated media. Automatically disable USB mass-storage functionality during normal operations.

Standards: NIST SP 800-171⁽³⁰⁾

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 3.

Guidance: RSUs generate operational logs, configuration data, diagnostic information, and security-relevant records that may be shared with internal teams or external entities such as vendors, system integrators, or oversight authorities. Improper sharing of this information could expose network architecture details, credential metadata, or configuration parameters that increase system risk.

The IOO defines policies governing when and how RSU information may be shared, including approval requirements, sanitization expectations, transmission protections, and recipient authorization. These policies apply to both internal sharing (e.g., between TMC and enterprise IT) and external sharing (e.g., vendor troubleshooting).

Information sharing controls may include restricting log exports to approved endpoints, enforcing encrypted transmission channels, limiting the scope of shared configuration data, and ensuring that certificate material or private key information is never disclosed. IP allow-listing, endpoint validation, or mutually authenticated TLS sessions may be used where data exchange occurs over IP networks.

Parameter Value(s):

paragraph a. “when sharing system logs, configuration data, audit records, or diagnostic reports containing security-relevant information with internal teams or external entities such as vendors.”

paragraph b. “automated access control decision tools, information labeling mechanisms, encrypted transmission channels, and documented user guidance procedures integrated into information-sharing workflows.”

AC-24, Access Control Decisions

Responsible Party (M/I): M/I

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

Guidance: Access control decisions for RSUs occur at multiple layers, including user authentication to management interfaces, role-based authorization for configuration functions, certificate validation for remote sessions, and PSID/SSP enforcement for V2X message transmission.

The IOO defines the access authorization information that must be evaluated before granting access to RSU functions. This includes user role assignments, device trust relationships, certificate status, and operational constraints such as maintenance windows or approved endpoints.

The manufacturer implements enforcement mechanisms within the RSU so that access decisions are evaluated before execution of sensitive actions. Enforcement applies to local console access, web or API-based management interfaces, remote sessions, firmware update functions, and security configuration changes. Access decisions are based on authenticated identity and associated privilege level, and are logged where appropriate.

Parameter Value(s):

#1 “Defined procedures and technical mechanisms for evaluating and enforcing access control decisions at the RSU and associated management systems.”

#2 “User or process authentication status, role-based authorization, certificate validity, and assigned privilege level.”

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: This control applies to both the IOO and RSU manufacturers or vendors.

The IOO establishes a structured role-based training program for personnel who manage, configure, maintain, monitor, or govern RSUs. Training content is aligned with job responsibilities and includes secure configuration practices, access control procedures, remote access handling, portable media

restrictions, incident reporting expectations, and the fundamentals of certificate-based trust used in V2X environments.

Personnel with administrative or security responsibilities receive additional instruction on certificate lifecycle management, firmware integrity validation, logging and monitoring practices, and enforcement of least-privilege principles. Training reinforces the distinction between V2X broadcast security (e.g., IEEE 1609.2 message authentication) and management-plane access control requirements.

Manufacturers ensure that development, integration, and support personnel receive comparable role-based training covering secure software development practices, configuration management, vulnerability handling, firmware signing processes, and secure deployment of RSUs within connected infrastructure environments.

Parameter Value(s):

paragraph a. “RSU manufacturers, integrators, administrators, field technicians, and network/security engineers.”

paragraph a.1. “annually”

paragraph b. #1: “annually”

paragraph b. #2: “After identification of new threats, vulnerabilities, or adversary TTPs relevant to RSUs 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): I

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

Guidance: The manufacturer provides RSU logging capabilities that record security-relevant and operationally significant events and, where applicable, expose audit and status information through supported NTCIP 1218 objects or equivalent management interfaces.

The IOO configures which event categories are enabled, defines retention and collection policies, and ensures logs are retrieved by the TMC or centralized monitoring system.

Event logging focuses on management-plane and security-relevant actions rather than V2X broadcast message payloads. At a minimum, logged events include authentication attempts to the

management interface, configuration and security parameter changes, firmware and software update actions, remote access session establishment and termination, certificate store modifications and CRL updates, changes to logging configurations.

NTCIP-managed RSUs should expose relevant audit and configuration state through standardized objects where supported, enabling centralized polling or event notification.

Parameter Value(s):

paragraph a. "RSU startup and shutdown; service and application startup, shutdown, and failure events; application and security configuration changes; network interface connection and loss events; successful and unsuccessful authentication attempts to management interfaces; software and firmware update attempts and outcomes; creation, modification, and deletion of user accounts and privilege assignments (where supported); changes to certificate stores, trust lists, or credential material; remote access session establishment and termination; changes to audit configuration; and attempts to modify or delete audit records. Logging of private key operation failures is included where technically feasible."

paragraph c. "all events defined in AU-2a"

paragraph e. "Review and update the defined event set 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

Standard: CTI 4001.⁽¹⁰⁾

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: Audit records include sufficient information to determine what event occurred, when it occurred, the source of the action (user ID, role, certificate identity, IP address, or interface), whether the action succeeded or failed. Where NTCIP 1218 is used, audit and status information should be represented through standardized object structures where feasible, supporting interoperability with TMC systems.

Where certificate-based authentication is used (e.g., remote access over TLS aligned with ISO 21177), audit records include certificate identity or endpoint information sufficient to correlate actions with authenticated entities.

Standard: NTCIP 1218⁽⁴⁷⁾, Section 3.5.1.1.7.3.5

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 control includes both technical capability and operational configuration.

The manufacturer provides sufficient on-device audit storage capacity and implements predictable rollover or overwrite behavior when storage limits are reached. The RSU supports configuration of logging levels and retention thresholds within the constraints of the device platform.

The IOO defines audit retention requirements at the program level and configures log transfer frequency, storage thresholds, and centralized collection processes accordingly. The RSU is not expected to serve as the long-term audit repository; instead, it retains logs locally only long enough to support operational continuity and reliable transfer to a centralized logging or monitoring system.

Where connectivity to centralized systems is temporarily unavailable, the RSU retains logs locally until successful transfer or until defined storage thresholds are reached.

Parameter Value(s):

“On-device audit storage sufficient to retain all defined audit events for a minimum of 7 days of normal operation or until successful transfer to a centralized logging system, whichever occurs first.”

Risk References and Resources:

ARC-IT Mechanisms: As specified in control.

ARC-IT Protocol Implementation Conformance (PIC) 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: Audit records generated by the RSU are transferred to a centralized logging or monitoring system, such as a TMC or enterprise security platform, to support retention, correlation, and incident response.

The manufacturer provides the capability for secure log export using authenticated and encrypted channels consistent with remote access and transmission security requirements. The RSU supports automated or scheduled transfer mechanisms and generates alerts when local storage utilization approaches defined thresholds.

The IOO defines the transfer frequency and retention requirements at the program level and ensures centralized systems are available to ingest and retain audit records. Where connectivity is temporarily unavailable, the RSU retains logs locally until successful transfer or until storage thresholds are reached.

Parameter Value(s):

"At least weekly, or immediately upon reaching a defined storage utilization threshold.

"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 RSU detects and reports failures in audit logging processes, including inability to record events, storage exhaustion, or failure to transmit logs to centralized systems.

The manufacturer provides mechanisms to detect audit subsystem failures and generate alerts locally and, where connectivity exists, remotely. The IOO defines who receives notifications and what operational response is required.

Where log transmission fails but local storage remains available, the RSU queues logs locally until connectivity is restored or storage thresholds are reached. Logging failures do not interfere with core V2X broadcast operations but are treated as security-relevant conditions requiring review.

Parameter Value(s):

paragraph a. #1 "Security administrators, Local Device Administrators, Remote Device Administrators"

paragraph a.#2 "Within one hour of detection."

paragraph b: " Queue logs locally and raise alert"

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: The RSU generates a warning when audit storage utilization reaches a defined threshold to prevent loss of security-relevant events due to log overwrite. Alerts are provided locally and, where connectivity exists, forwarded to centralized monitoring systems.

The IOO defines alert recipients and threshold values within the configurable capabilities provided by the manufacturer.

Parameter Value(s):

#1 "Local device administrators", "Security administrators"

#2 "1 hour"

#3 "80%"

AU-5(2), Response to Audit Logging Process 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 RSU provides timely alerts for critical audit processing failures, including audit subsystem errors, failure to record events, and storage capacity exhaustion. Where connectivity to centralized systems exists, alerts are transmitted without undue delay.

Parameters:

#1 “Security administrators and designated RSU administrators.”

#2 “Near real-time, not to exceed 15 minutes where connectivity permits.”

#3 “At minimum: audit software or hardware errors, failure of audit capture mechanisms, and storage capacity reaching or exceeding defined thresholds.”

Risk References and Resources:

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 reviewing and analyzing RSU audit records to detect unauthorized access, configuration changes, certificate or trust store modifications, firmware updates, or abnormal remote access activity. Review processes focus on management-plane and security-relevant events rather than V2X broadcast message traffic.

Audit review includes logs generated locally by the RSU and logs forwarded to centralized systems such as a TMC or enterprise monitoring platform. The IOO defines which event categories require periodic review, which require near real-time monitoring, and how findings are escalated.

Special attention is given to connections between the RSU and back-office systems, TMS platforms, maintenance laptops, or other external systems, particularly where remote access or certificate-based authentication is used.

Parameter Value(s):

paragraph a.1 “At least quarterly for formal review of aggregated audit records.”

paragraph a.2. “Minimally: failed authentication attempts, remote access session activity, firmware or configuration changes, certificate or trust store modifications, system and application failures.”

paragraph b. “Designated administrators or security personnel.”

Risk References and Resources:

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: Audit records generated by RSUs are included in centralized review and analysis processes where connectivity permits. The IOO defines which RSU services and interfaces are in scope for centralized monitoring, including management interfaces, remote access sessions, certificate lifecycle events, and firmware updates.

Central review may be performed through a TMC logging platform, enterprise SIEM, or equivalent monitoring system. The objective is correlation across multiple RSUs and related infrastructure to detect coordinated or anomalous activity.

Connections to back-office systems, TMS platforms, maintenance laptops, and other authorized external systems are included in centralized analysis where technically feasible.

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: Where RSUs are deployed in roadside cabinets or other physically accessible environments, audit records are correlated with physical monitoring events when such capabilities exist. This may include cabinet door open sensors, tamper switches, enclosure intrusion detection, or loss of power events.

The manufacturer provides the capability to log tamper or enclosure-related events where supported by the hardware platform. The IOO determines how physical event logs are reviewed and correlated with administrative or configuration changes to detect potential compromise.

AU-7, Audit Record Reduction and Report Generation | Integrated Analysis 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: Audit records generated by RSUs are aggregated and analyzed in a manner that supports identification of anomalous behavior across devices and interfaces. Because RSUs are edge devices with limited on-board analysis capability, integrated analysis typically occurs at a centralized system such as a TMC logging platform or enterprise monitoring system.

The IOO defines the conditions under which audit records are reviewed, reduced, and summarized into reports. This includes identifying event patterns that warrant escalation, such as repeated authentication failures, unauthorized configuration attempts, unexpected firmware updates, certificate or trust store modifications, or coordinated activity across multiple RSUs.

The manufacturer supports this control by ensuring audit records can be exported in a structured format suitable for centralized analysis and reporting.

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: Audit information generated by the RSU is protected against unauthorized access, modification, or deletion. Protection applies both to logs stored locally on the RSU and to logs transmitted to centralized systems.

The manufacturer provides mechanisms to restrict access to audit records to authorized roles and to prevent unauthorized modification or deletion of logs. Access to audit information is limited to designated administrative or security roles consistent with least-privilege principles.

The IOO defines which roles are authorized to access audit records and establishes procedures for reviewing and responding to suspected tampering. Attempts to modify logging configuration or delete audit records are themselves logged and treated as security-relevant events.

Parameter Value(s):

paragraph b. "Local device Administrators, Security Administrators"

Risk References 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: Because RSUs are field-deployed devices with limited storage and potential physical exposure, audit records are periodically transferred to a separate, centralized system such as a TMC logging platform, enterprise monitoring system, or other designated repository.

The manufacturer provides the capability to export audit records securely to an external system. The IOO defines transfer frequency and centralized retention requirements. The RSU is not intended to serve as the authoritative long-term audit repository.

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: Audit records are protected against undetected modification using cryptographic integrity mechanisms. The manufacturer implements mechanisms such as digital signatures, keyed hashes, or secure hashing (e.g., SHA-256 or stronger) to provide tamper-evident protection for stored or transmitted logs.

Where logs are transmitted to centralized systems, integrity and confidentiality protections are applied using authenticated and encrypted channels consistent with AC-17 and applicable standards (e.g., TLS aligned with ISO 21177 where used for ITS station connectivity).

Cryptographic mechanisms are implemented using FIPS 140-3 validated modules where required by organizational policy.

Risk References and Resources:

ARC-IT Mechanisms: See control AU-09.

Standard: FIPS 140-3

AU-11, Audit Record Retention

Responsible Party (M/I): M/I

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

Guidance: Audit records generated by RSUs are retained in accordance with organizational retention policies and applicable regulatory or legal requirements. Because RSUs are field-deployed edge devices with limited storage capacity, long-term retention is performed in centralized logging or monitoring systems rather than on the RSU itself.

The manufacturer provides the capability for local audit storage sufficient to support disconnected operations and reliable transfer to centralized repositories. The RSU supports secure export of audit records using authenticated and encrypted channels consistent with remote access and transmission security controls.

The IOO defines retention periods at the program level and ensures centralized systems retain audit records for the required duration. Where RSUs operate temporarily offline, logs are retained locally until connectivity is restored or defined storage thresholds are reached.

Parameter Value(s):

"Retain audit records in centralized repositories for a minimum of three years; retain audit records locally on the RSU only until successful transfer or until storage thresholds are reached."

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 RSU sufficient to support the event categories defined under AU-02. The RSU is capable of generating audit records for authentication attempts to management interfaces, including both successful and unsuccessful events; configuration and security setting changes; firmware and software update attempts and outcomes; establishment and termination of remote access sessions; account and privilege changes where supported; modifications to certificate stores, trust lists, or other credential material; changes to audit configuration; and attempts to modify or delete audit records.

Audit generation applies to management-plane and security-relevant functions across supported interfaces, including local console access, web-based or API management interfaces, remote access mechanisms, and security configuration components. Logging of individual V2X broadcast message payloads is not required, as broadcast integrity and authentication are handled at the message layer under IEEE 1609.2 rather than through management-plane auditing.

Parameter Value(s):

paragraph a. “RSU operating system (where applicable), application layer, management interfaces, communications interfaces, and security functions.”

paragraph b. “Audit administrator or designated RSU 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 provides the capability to modify audit logging configuration only by authorized roles. Changes to logging parameters, event categories, or severity thresholds are themselves logged.

Logging configuration changes are restricted to designated administrative roles. The RSU ensures that audit generation for critical security events cannot be completely disabled without explicit administrative action, and that such actions are recorded.

Parameter Value(s):

#1 “Local device administrator, Audit administrator”

#2 “RSU operating system and application layer, communications interfaces, maintenance interfaces, and security functions”

#3 “Event severity or type, operational mode, interface, or temporal criteria”

#4 “Five minutes of authorized change initiation for local console sessions; ten minutes of

authorized change initiation for remote administrative sessions; immediately upon reboot or system reset"

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

Guidance: The IOO establishes monitoring processes to detect potential unauthorized disclosure of RSU operational, configuration, audit, or credential-related information. Monitoring applies to external connections between the RSU and TMC systems, back-office systems, vendor support platforms, and maintenance devices. Particular attention is given to log export activity, configuration data transfers, certificate or trust store modifications, and unexpected outbound communications.

The IOO defines how suspected information disclosure events are identified, escalated, and investigated. Where compromise of credentials or certificates is suspected, response actions include revocation or reissuance of affected credentials and coordination with relevant stakeholders.

Parameter Value(s):

paragraph a. #1 "Monitoring of outbound management communications, log export activity, configuration data transfers, and certificate or credential-related events."

paragraph a. #2 "At least weekly review of relevant audit records, and immediate review upon detection of anomalous activity or suspected compromise."

paragraph b. #1 "Security administrators, system administrators, and incident response personnel."

paragraph b. #2 "Initiate incident response procedures, assess impact to RSU operations and credentials, revoke or reissue affected certificates or keys where necessary, and notify impacted external entities as required."

AU-16, Cross-Organizational Audit 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 establishes documented mechanisms to coordinate logging, monitoring, and incident response with external organizations. This may include TMC systems operated by a different authority, managed service providers, or ITS partners participating in shared infrastructure.

Audit data exchanged across organizational boundaries is transmitted using authenticated and encrypted mechanisms consistent with remote access and transmission security controls. Where IP-based communication between ITS stations is used, implementations may align with applicable secure communication profiles.

The manufacturer provides the capability to generate audit records that include sufficient identity information to support cross-organizational traceability, including user identity, certificate identity, or authenticated endpoint information where applicable.

Parameter Value(s):

#1 “Authenticated and encrypted data exchange mechanisms for cross-organizational audit transmission.”

#2 “Security-relevant event logs, remote access records, configuration and firmware change events, and certificate or credential management events.”

Standards: NIST SP 800-52⁽⁴⁶⁾

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 formally approves and documents all systems and organizational entities that exchange information with the RSU across authorization boundaries. For RSUs, this typically includes transportation management systems (TMS), back-office or cloud platforms, maintenance and vendor support systems, roadside gateways, and, where applicable, certificate management or SCMS-related infrastructure.

Information exchanges are documented through interconnection security agreements or equivalent information exchange agreements that define the purpose of the connection, data types exchanged, authentication mechanisms, cryptographic protections, logging expectations, and incident response coordination. Exchanges occurring over IP networks use authenticated and encrypted mechanisms consistent with remote access and transmission security controls, and where applicable may align with ISO 21177 profiles for secure ITS station communications.

V2X broadcast communications are distinguished from management-plane interconnections. Broadcast safety messages are intentionally receivable by compliant ITS stations and rely on IEEE 1609.2 message-layer authentication rather than bilateral interconnection agreements. Management and control-plane communications, by contrast, require explicit authorization and documentation.

Parameter Value(s):

paragraph a. “Interconnection security agreements or documented information exchange security agreements defining purpose, data types, authentication mechanisms, cryptographic protections, logging responsibilities, and incident response coordination.”

paragraph c. “Annually, and upon significant configuration, system, or organizational changes affecting the information exchange.”

Risk References and Resources:

NIST SP 800-82: Organizations perform risk-benefit analysis to determine whether an ITS should

be connected to other systems. The authorizing official (AO) 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 Authorizations

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 pre-authorizes individuals, roles, and systems permitted to exchange information with the RSU management interfaces. Authorization decisions are based on defined operational need, authenticated identity (user or device), and documented trust relationships.

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 resulting from approved RSU interconnections. This includes downstream systems indirectly reachable through direct connections, such as centralized TMS platforms, vendor-managed service environments, or partner ITS infrastructure.

Risk assessments consider how data exchanged with one system may be further transmitted, stored, or processed by other systems outside the original authorization boundary. Where security controls of downstream systems cannot be validated or contractual protections are insufficient, information exchanges are re-evaluated or restricted.

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 maintains a plan of action and milestones (POA&M) to document identified weaknesses in RSU deployments, including unimplemented or partially implemented security controls, configuration gaps, software defects with security impact, and unresolved vulnerabilities.

The POA&M is used to track remediation activities, assign responsibility, establish timelines, and document risk acceptance decisions where corrective action cannot be immediately completed. This includes weaknesses identified during procurement, integration, security assessments, vulnerability scanning, incident response, or vendor disclosures.

Where security deficiencies originate from the RSU platform or firmware, the IOO coordinates with the manufacturer or integrator to obtain remediation plans and expected resolution timelines. Compensating controls may be implemented to reduce risk while permanent fixes are pending.

Parameter Value(s):

“Reviewed and updated at least quarterly, and whenever new weaknesses are identified or existing items are remediated.

”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 "Compromise organizational information systems to facilitate exfiltration of data/information" in table 3, Exploit and Compromise.

Guidance: The IOO designates a senior official or accountable authority responsible for approving the operation of RSUs based on an understanding of cybersecurity risks. Authorization decisions consider identified vulnerabilities, open POA&M items, interconnections with external systems, certificate and credential management practices, remote access controls, and operational impact to transportation safety.

Risk acceptance decisions are documented and revisited periodically or when significant changes occur, such as major configuration changes, firmware updates, new interconnections, or changes in threat conditions.

Parameter Value(s):

paragraph e. “At least annually, and upon significant system, configuration, interconnection, or threat changes.”

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 maintains a continuous monitoring strategy for RSU deployments that supports timely detection of security-relevant events, changes in system posture, and emerging risks. Continuous monitoring focuses on management-plane and security-related activities and is coordinated with centralized logging and incident response processes.

Monitoring includes review of authentication activity, remote access sessions, configuration and firmware changes, certificate or trust store modifications, audit subsystem status, and abnormal communication patterns between the RSU and authorized external systems.

Parameter Value(s):

paragraph a. "Authentication activity, remote access sessions, configuration and firmware changes, certificate or trust store modifications, audit subsystem health, and anomalous communication patterns."

paragraph b. #1 "Near-real-time where technically feasible for critical security events; otherwise daily."

paragraph b. #2 "Weekly review of aggregated monitoring data."

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

paragraph g. #2 "Daily review of critical security alerts."

Risk References and Resources:

NIST SP 800-82: 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(4), Continuous Monitoring | Risk 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 defines metrics and evaluation criteria to assess the effectiveness of implemented risk response measures for RSUs. This includes validation that encryption mechanisms for management-plane communications remain properly configured, certificate lifecycle processes are functioning as intended, remote access controls are enforced, and logging mechanisms remain operational.

Risk monitoring includes reassessment when significant changes occur, such as firmware updates, new interconnections, certificate renewals, or updated threat intelligence relevant to RSU deployments.

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 defines the level of automation required to support timely and accurate monitoring of RSU security posture. Automated mechanisms may include centralized log collection systems, configuration compliance monitoring tools, vulnerability scanning platforms, and alerting dashboards.

The manufacturer provides the capability for the RSU to export logs, status information, and configuration data in formats suitable for automated ingestion and analysis.

Parameter Value(s):

“Automated log collection and analysis tools, configuration compliance monitoring, vulnerability scanning mechanisms where technically feasible, and centralized alerting dashboards integrated into the continuous monitoring process.”

CA-8, Penetration Testing

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. 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: Penetration testing of RSUs is a shared responsibility between the IOO and the manufacturer. The IOO conducts or commissions penetration testing to assess the effectiveness of deployed security controls within its operational environment. The manufacturer supports this effort by providing necessary technical documentation, test configurations, and remediation of identified vulnerabilities within the RSU platform, firmware, or hardware components.

Penetration testing evaluates both management-plane and device-level attack surfaces. Testing may include attempts to bypass authentication mechanisms, escalate privileges, exploit exposed services, manipulate firmware update processes, interfere with certificate validation or trust stores, abuse remote access mechanisms, or extract sensitive configuration or credential material. Where applicable, testing may also assess the resilience of wireless management interfaces and cellular backhaul connectivity.

Because RSUs are field-deployed and safety-adjacent devices, penetration testing is conducted in a controlled manner that does not interfere with active traffic operations. Testing is performed in laboratory environments, staging networks, replicated environments, or scheduled maintenance windows. Production devices are not subjected to disruptive testing without coordination and documented risk acceptance.

Results of penetration tests are documented, tracked through the POA&M process, and remediated or mitigated based on risk and operational impact.

Parameter Value(s):

#1 "At least annually, and after significant firmware updates, architectural changes, or newly disclosed critical vulnerabilities."

#2 "management interfaces (web, API, SSH), remote access mechanisms (TLS/VPN), certificate and credential storage, firmware update mechanisms, configuration interfaces, exposed network services, wireless management interfaces, cellular backhaul connectivity, debugging and maintenance ports (e.g., UART, JTAG), and physical tamper resistance controls."

Risk References and Resources:

NIST SP 800-82: 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⁽²⁸⁾

CA-9, Internal System Connections

Responsible Party (M/I): M/I

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

Guidance: Internal system connections within and around the RSU are defined, documented, and authorized. This includes logical connections between RSU subsystems (e.g., application processor, communication modules, security modules), as well as physical or network connections to other components within the roadside cabinet or field environment.

The IOO documents which internal and cabinet-level connections are permitted and the purpose of each connection. Authorization may be granted for specific components or for defined classes of components based on shared characteristics such as protocol type, interface standard, or baseline configuration.

The manufacturer provides architectural documentation identifying internal interfaces, exposed service ports, communication pathways between subsystems, and supported external interface types. Where feasible, the RSU enforces logical separation between management-plane functions, V2X radio functions, and other internal components to reduce lateral movement risk.

Connections that are not required for operational purposes are disabled or physically removed. Debugging or maintenance interfaces that are not intended for routine use are restricted, disabled, or protected through access controls.

Parameter Value(s):

paragraph a. "Authorized connections between the RSU and cabinet-level components, including the Traffic Signal Controller (TSC), Roadside Cabinet Electronics (RSCE), Transportation Field Cabinet System (TFCS), sensors, power modules, and network infrastructure devices."

paragraph c. Upon device decommissioning, network reconfiguration, integration of new components, detection of security incidents, or when a connection is no longer operationally required.”

paragraph d. " "At least semi-annually, and upon significant architectural or configuration changes.”

Risk References and Resources:

NIST SP 800-82: Organizations perform risk-benefit analysis to determine whether ITS equipment should be connected to other internal system components and then document those connections. The AO fully understands the potential risks associated with approving individual connections or approving a class of components to be connected. For example, the AO may broadly approve the connection of any sensors limited to 4 to 20 milliamp (mA) 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): 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 maintains a documented baseline configuration for deployed RSUs. The baseline includes approved firmware versions, enabled services, network interface settings, V2X radio parameters, certificate trust anchors, cryptographic configurations, access control settings, logging configuration, and remote access policies.

The baseline reflects both operational requirements and security controls and serves as the reference state for detecting unauthorized or unintended configuration changes. Baseline definitions are aligned with applicable standards, including CTI 4001, SCMS enrollment security requirements, and organizational policies.

Parameter Value(s):

paragraph b.1 “Annually, and upon major firmware or architectural change.”

paragraph b.2 “Significant system changes, security incidents, or vendor-released critical security patches.”

Standard: CTI 4001⁽³⁷⁾, Section 3.3.3.1

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 uses a documented change control process for RSU deployments that covers approval, scheduling, validation, and rollback planning prior to making changes in the field. This

process is typically executed through the TMC, a centralized device management platform, or integrator-maintained procedures rather than directly on the RSU.

The manufacturer supports change control by providing RSU capabilities that allow configuration changes to be made through authenticated management interfaces and by generating audit evidence of changes where feasible.

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: Prior to implementing significant configuration or firmware changes to RSUs, the IOO conducts an impact analysis to assess potential cybersecurity, safety, operational, and interoperability effects. Impact analysis considers certificate validity, trust relationships, remote access posture, logging continuity, and potential effects on V2X message integrity and timing.

Where applicable, safety and signal operations personnel are included in change review to ensure that modifications do not adversely affect traffic control functionality or emergency response capabilities.

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 RSU configuration functions. Only authorized personnel may initiate firmware updates, certificate installation, network configuration changes, or modification of V2X operational parameters.

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: Dual authorization is required for high-risk configuration changes that could materially impact RSU security posture or operational safety. This includes firmware image deployment, modification of message configuration files affecting signal behavior, installation or replacement of SCMS certificates, changes to trust anchors, and modification of cryptographic policies.

Parameter Value(s):

"firmware images and MAP/SPaT data files, SCMS certificates"

CM-6, Configuration Settings

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. 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 defines required secure configuration settings for RSUs based on operational needs and applicable standards. These settings include network interface restrictions, cryptographic protocol requirements, certificate validation behavior, access control configurations, radio parameters, and logging requirements.

The manufacturer implements configurable settings within the RSU that allow enforcement of these security parameters and ensures that such settings are modifiable only by authorized roles. Default configurations support secure deployment, including denial of unnecessary services, enforcement of modern cryptographic protocols, certificate validation and revocation checking, secure boot and signed firmware validation, and authenticated time synchronization.

Parameter Value(s):

paragraph a. “Organization-defined secure configuration settings for RSUs, including: C-V2X channel plan and transmit power; deny-all/allow-list of services and ports; TLS 1.3 with NIST-approved cipher suites; SCMS certificate validation and revocation checking; default account disablement and RBAC; secure boot and signed-firmware enforcement; authenticated time sync (NTP/IEEE-1588); audit logging levels/targets; management interface restrictions (e.g., SSHv2 key-based only, no Telnet); and FIPS-mode enablement where supported.”

paragraph c. #1 “RSUs, integrated V2X radio modules within RSUs, and roadside backhaul gateways/routers directly interfacing with RSUs.”

paragraph c. #2 “Continuity of safety messaging (e.g, BSMs) under latency/availability constraints; time-bounded field maintenance and recovery operations; interoperability dependencies with TMC/SCMS; and emergency operations requiring temporary configuration exceptions (with documented justification and reversion plan).”

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).

Guidance: RSUs are deployed as purpose-built field devices and are configured to provide only the functions necessary to support authorized V2X messaging, secure management, and approved backhaul communications. Unnecessary services, protocols, ports, and software components are disabled or not included in the deployed configuration.

The IOO defines which operational capabilities are required for its deployment environment, including approved V2X applications, backhaul connectivity methods, and management interfaces. The manufacturer designs the RSU platform to minimize exposed services by default and to allow unused services and interfaces to be disabled.

Least functionality applies to management-plane interfaces, operating system services (where applicable), wireless management interfaces, and physical debugging ports.

Parameter Value(s):

paragraph a. "SAE J2735 message broadcasting (e.g., MAP, SPaT, TIM, RSM), certificate validation and revocation checking, and secure backhaul communications to authorized TMC or SCMS systems."

paragraph b. "Unnecessary network services and ports; Telnet or insecure management protocols; unused wireless management interfaces; and debugging interfaces (e.g., JTAG, UART) unless explicitly authorized for maintenance."

Risk References and Resources:

NIST SP 800-82: 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

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 RSU platform restricts execution of unauthorized programs or scripts. Where the RSU operating environment supports application execution, only digitally signed and manufacturer-approved software components are permitted to run.

Auto-execution features (e.g., from removable media or uploaded files) are disabled unless explicitly required for controlled maintenance activities. Firmware update processes enforce digital signature validation prior to execution.

The IOO defines policies governing approved software use and maintenance procedures. The manufacturer ensures that the RSU platform does not permit arbitrary code execution by field users.

Parameter Value(s):

“Execution restricted to digitally signed firmware and authorized system components; automatic execution from removable media or uploaded content disabled by default.”

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 RSU enforces a deny-by-default policy for software execution. Only authorized and validated firmware, application modules, and supporting components are permitted to execute. Installation or execution of non-approved V2X applications or third-party software is prohibited.

The IOO maintains visibility into approved firmware versions and application sets. T

Parameter Value(s): “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 RSU executes only explicitly authorized software components. Authorized components typically include the operating system kernel (where applicable), signed firmware images, management services, certificate and credential management modules, cryptographic libraries, and required network communication services.

The IOO maintains an inventory of approved firmware and software versions for deployed RSUs. Changes to the authorized software set are controlled through configuration management procedures.

Parameter Value(s):

paragraph a. “Operating system kernel (where applicable), digitally signed firmware images, management services, credential and certificate management modules, cryptographic libraries, and required network communication services.”

paragraph c. “at least annually”

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 which hardware components are authorized to interface with the RSU, including radio modules, storage devices, network modules, and maintenance equipment. Unauthorized hardware components, peripheral devices, or field modifications are not permitted.

The manufacturer designs the RSU to restrict unauthorized hardware connections where feasible, including disabling unused USB ports, restricting peripheral interfaces, and protecting debugging or expansion interfaces.

Parameters:

paragraph c. “at least annually”

CM-8, System Component Inventory

Responsible Party (M/I): I

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

Guidance: The IOO maintains an inventory of RSU system components sufficient to support configuration management, vulnerability management, lifecycle tracking, and incident response. The inventory includes deployed RSU devices and relevant subcomponents that affect security posture, such as integrated V2X radio modules, firmware versions, cryptographic modules, management interfaces, and associated roadside networking equipment.

Inventory records enable the IOO to determine which RSUs are affected by newly disclosed vulnerabilities, firmware updates, certificate lifecycle events, or configuration changes. For field deployments, inventory records also include physical deployment location and cabinet association to support operational coordination and incident response.

The inventory may be maintained within a centralized asset management system, device management platform, or configuration management database. Inventory accuracy is verified periodically and whenever components are installed, replaced, upgraded, or decommissioned.

Parameter Value(s):

paragraph a.5. “Unique device identifier; physical location; hardware model and serial number; firmware and software version; integrated radio module type; cryptographic module version (where applicable); and date of last firmware or configuration change.”

paragraph b. “Semi-annually, and immediately following component installation, replacement, upgrade, or decommissioning.”

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 and maintains a configuration management plan applicable to RSU deployments. The plan defines roles and responsibilities for managing RSU hardware, firmware, configuration settings, and associated roadside networking components. It establishes procedures for baseline maintenance, change control, version tracking, firmware updates, rollback procedures, and configuration verification.

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: RSUs operate using manufacturer-provided firmware and approved software components only. The IOO ensures that only authorized firmware versions and application modules are deployed and that unsupported or unapproved software components are not introduced into the RSU environment.

Software usage restrictions apply primarily to firmware images, management utilities, and configuration tools used in conjunction with the RSU. The IOO maintains visibility into deployed firmware versions and ensures updates are obtained from authorized sources.

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: RSUs are designed to prevent installation of arbitrary user-supplied software. Software installation is limited to manufacturer-provided firmware or authorized update packages delivered through controlled and authenticated mechanisms.

The IOO defines policy governing who is authorized to initiate firmware updates or approved software installations. The manufacturer implements enforcement mechanisms such as hardware-backed secure boot, digital signature validation for firmware images, restricted maintenance interfaces, and role-based access control limiting update privileges.

Once deployed, the IOO monitors compliance through logging and configuration review processes. Any deviation from authorized firmware or software versions is investigated.

Parameter Value(s):

paragraph a. "Hardware-enforced secure boot; digital signature validation of firmware images; restricted or disabled debugging interfaces (e.g., JTAG, UART) post-deployment; and update mechanisms requiring certificate-based authentication."

paragraph b. “Role-based access control restricting firmware installation privileges to authorized administrative roles.”

paragraph c. “Continuous automated logging of firmware installation attempts, with periodic review at least monthly.”

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: Installation of firmware or authorized software components on the RSU requires authenticated administrative privileges. Privilege requirements align with defined role-based access control policies and are enforced by the RSU platform.

Firmware installation processes validate both the identity of the initiating user or endpoint and the digital signature of the update package prior to execution. Unauthorized users are not permitted to initiate software installation.

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: RSUs back up configuration and security-relevant state necessary to restore the device to an operational and trusted condition. Full device image backups are not required.

The IOO defines required backup elements and retention. The manufacturer ensures the RSU supports secure export of configuration and logs through authenticated and encrypted management interfaces.

Device-unique private signing keys are not exported. If key material is lost or compromised, the device is reprovisioned or re-enrolled rather than restored from plaintext key backup.

Parameter Value(s):

paragraph a. #1 “Configuration settings; radio and application parameters; certificate trust store (excluding non-exportable private keys); enrollment or provisioning metadata; and audit logs.”

paragraph a. #2 “Weekly and prior to firmware or significant configuration updates.”

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

paragraph c. “Upon configuration change, firmware update, or certificate lifecycle event.”

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 periodically verifies that exported configuration backups and associated recovery procedures are usable and accurate. Testing may include restoration to a lab or spare RSU, configuration comparison validation, or cryptographic hash verification of backup artifacts.

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-9(8), System Backup | Cryptographic Protection

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: Backup data exported from the RSU is protected in transit and at rest using organization-approved cryptographic mechanisms. Sensitive backup elements include configuration files containing security settings, certificate trust anchors, enrollment metadata, and audit logs.

Private cryptographic keys used for message signing or device identity are protected within secure hardware modules where supported and are not exported in plaintext form. Where recovery of device identity is required, reprovisioning procedures are used rather than raw key restoration.

Parameter Value(s):

“Configuration backups, certificate trust stores, enrollment metadata, and audit logs are protected using approved cryptographic mechanisms; device-private signing keys remain hardware-protected and non-exportable.

”Standards: FIPS 197⁽³⁵⁾

CP-10, System Recovery and Reconstitution

Responsible Party (M/I): 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 to restore RSUs to a known secure state following hardware failure, compromise, or configuration corruption. Recovery procedures may include firmware reinstallation, configuration restoration from validated backups, certificate re-enrollment, and verification of secure boot and trust store integrity.

Recovery procedures ensure that restored RSUs resume authorized V2X operations only after configuration integrity, certificate validity, and network connectivity have been verified. Where device replacement is more practical than in-place restoration, reconstitution procedures include secure provisioning of replacement hardware.

Parameter Value(s):

“Target recovery or replacement within 24 hours for critical deployments, or as defined in the contingency plan.

”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 RSU supports identification and authentication across three distinct security domains: management-plane user access, network-level system connectivity, and V2X message-layer trust. The IOO defines authentication requirements appropriate to each domain. The manufacturer implements mechanisms to enforce those requirements within the RSU platform.

Application to Management Plane (User Authentication): All users accessing RSU management interfaces (for example the local console, web interface, API, SSH, or remote maintenance sessions) are uniquely identified and authenticated. Shared administrative accounts are not permitted unless explicitly justified and compensating controls (e.g., enhanced auditing) are implemented.

Authentication methods may include passwords, cryptographic tokens, client certificates, or hardware-backed credentials. Authentication strength aligns with user privilege level.

Application to Network Plane (Device/System Authentication): When the RSU establishes management or backhaul communications with TMC systems, gateways, or other infrastructure, mutual authentication is performed using certificate-based mechanisms. TLS sessions are established using device-unique credentials issued under an approved trust domain and validated prior to communication. Where ISO 21177 profiles are applicable for secure ITS station-to-station communications, authentication requirements align with those profiles. Device authentication is logically separate from V2X broadcast authentication.

Application to V2X Plane (Message Authentication): V2X broadcast messages are not authenticated through user login or TLS session establishment. Instead, message authenticity and integrity are enforced at the message layer using IEEE 1609.2 security services.

Each outbound message is digitally signed using a valid application certificate. Receiving entities validate certificate chains, PSID authorization, SSP constraints, and revocation status prior to processing the message.

Risk References and Resources:

NIST SP 800-82:⁽³⁾ When 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.

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: Privileged users such as administrators, engineers, and personnel authorized to perform configuration changes, firmware updates, certificate management, or security policy modifications are uniquely identified and authenticated using multifactor authentication when accessing RSU management interfaces. Remote privileged access, whether through backhaul connectivity, VPN, TLS-based management sessions, or maintenance laptops connected over IP, requires multifactor authentication without exception. For local console access within a physically secured roadside cabinet, physical access controls (e.g., locked enclosures, controlled keys, secured maintenance ports) may serve as one authentication factor when permitted by organizational policy. All privileged access events are logged for accountability.

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: Non-privileged users who access RSU management or monitoring interfaces are uniquely identified and authenticated. Multifactor authentication is required where technically feasible and consistent with operational constraints.

Although non-privileged users typically perform monitoring or limited operational functions, authentication mechanisms must preserve accountability, session integrity, and traceability of actions.

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: RSUs are uniquely identified and authenticated when establishing network-based communications with other infrastructure components. Device authentication is distinct from user authentication and distinct from V2X message-layer authentication.

For management-plane and backhaul communications, the RSU authenticates to authorized infrastructure systems (e.g., TMCs, roadside gateways, cloud services) using certificate-based mutual authentication. Device identity is bound to cryptographic credentials issued under an approved trust domain. Where applicable, secure communications profiles align with ISO 21177 TLS-based ITS station security specifications. Unauthenticated network connectivity to management or back-office systems is not permitted.

For V2X communications, device trust is established through compliance with IEEE 1609.2 security services and SCMS enrollment processes. Each RSU obtains and maintains enrollment and operational certificates in accordance with SCMS requirements. Message authentication is performed at the application layer through digital signatures. Receiving entities validate certificate chains, PSID authorization, SSP constraints, and revocation status prior to processing messages.

The IOO maintains authoritative records of device identity, certificate status, and trust domain participation. The manufacturer ensures that the RSU platform securely stores device credentials, protects private keys from extraction, and supports certificate lifecycle operations, including enrollment, renewal, and revocation handling consistent with SCMS requirements.

Parameter Value(s):

#1 “All RSUs and any integrated or associated ITS stations that participate in authenticated network communications or SCMS enrollment processes.”

#2 “Management-plane TLS sessions, backhaul communications, and V2X certificate-based message authentication processes.”

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 “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 policies governing the generation, distribution, storage, renewal, revocation, and replacement of authenticators used by RSUs, aligned with applicable Certificate Policies (CP), Certification Practice Statements (CPS), SCMS requirements, and organizational security policy where PKI is involved. The manufacturer designs and implements RSU capabilities that enforce those policies and certificate management requirements.

For management access, the IOO defines allowable authenticators such as passwords, client certificates, or hardware-backed credentials and establishes requirements consistent with NIST SP 800-63B and applicable organizational policy. The manufacturer ensures the RSU securely stores authenticators, transmits them only over cryptographically protected channels, and removes all default credentials prior to deployment. The IOO requires immediate revocation of authenticators upon suspected or confirmed compromise, and the manufacturer ensures the RSU supports prompt revocation, replacement, and audit logging of those events.

For secure network communications, the IOO defines device identity and certificate requirements for TLS-based management and backhaul sessions, aligned with applicable Certificate Policies and ISO 21177 where implemented. The manufacturer provisions each RSU with device-unique X.509 or IEEE Std. 1609.2 credentials and enforces mutual authentication for TLS sessions. The manufacturer protects associated private keys within validated cryptographic modules or hardware-backed secure storage and prevents plaintext export. The IOO governs certificate issuance, renewal, suspension (where supported), and revocation in accordance with the applicable PKI Certificate Policy and Certification Practice Statement.

For V2X operations, the IOO enrolls RSUs into an SCMS-compliant public key infrastructure consistent with IEEE 1609.2, IEEE 1609.2.1, and applicable SCMS enrollment and end-entity security requirements. The manufacturer ensures the RSU supports Enrollment Certificate acquisition, secure generation or storage of associated private keys, and provisioning of application certificates for message signing. The RSU digitally signs outbound V2X messages using valid certificates and validates inbound certificates by constructing certification paths to trusted SCMS root authorities identified through the current Certificate Trust List. The manufacturer implements Certificate Revocation List processing and enforces revocation status checking prior to accepting signed messages. The IOO contracts with an SCMS that manages distribution and update of Certificate Trust Lists, trust anchors, and CRLs in accordance with SCMS Certificate Policy requirements, and the manufacturer ensures the RSU processes and applies those updates securely and without

unauthorized modification. Where separate PKI domains are used for management-plane and SCMS communications, the IOO defines trust separation requirements consistent with applicable Certificate Policies, and the manufacturer enforces logical and cryptographic separation of trust stores.

Parameter Value(s):

paragraph f. #1 “Prior to expiration in accordance with applicable Certificate Policy (CP), Certification Practice Statement (CPS), or organizational authenticator policy; no arbitrary periodic rotation absent risk-based justification.”

#2 “Upon suspected or confirmed compromise, device decommissioning, trust anchor change, or revocation notification.”

Risk References and Resources:

ATT&CK for ICS Mitigations / Techniques:

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

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

ARC-IT Mechanisms:

Device shall store encrypted hashed passwords in a database (only accessible to privileged users) using a strong encryption algorithm.

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

Standards: NIST SP 800-63B⁽³⁶⁾, IEEE 1609.2.1.⁽¹⁹⁾

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, Section *Configuration and Maintenance Vulnerabilities and Predisposing Conditions*.

Guidance: This control applies to both the IOO and the manufacturer. The IOO determines whether password-based authentication is permitted for RSU management access and defines password policy requirements consistent with NIST SP 800-63B and organizational risk tolerance. Where passwords are permitted, the IOO requires screening of new passwords against lists of commonly used, expected, or compromised values and defines the specific conditions under which password

changes are required, such as suspected or confirmed compromise, role change, or other policy-defined events.

The manufacturer ensures that when password-based authentication is supported, authentication exchanges occur only over cryptographically protected channels (e.g., TLS or SSH). The RSU stores passwords using salted, one-way cryptographic hash functions within protected storage and prevents retrieval of plaintext credentials. The manufacturer removes or disables all default credentials prior to deployment and enforces minimum length and blocklist screening requirements. The RSU provides secure mechanisms for password change and reset, and logs password-related administrative events consistent with applicable audit controls.

Parameter Value(s):

paragraph a. “at least quarterly and upon receipt of new threat intelligence, breach notifications, or relevant vulnerability disclosures.”

paragraph h. “Minimum length of at least 12 characters; allow all printable ASCII and Unicode characters;

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⁽³⁶⁾

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: RSUs rely on public key-based authentication for both V2X message security and management or backhaul communications. The IOO enrolls RSUs with an SCMS provider and, where applicable, with an enterprise X.509 PKI provider. The governing Certificate Policy (CP) and Certification Practice Statement (CPS) are established by those PKI providers. The IOO ensures RSUs operate in accordance with the applicable CP and CPS requirements.

For V2X operations, the manufacturer ensures the RSU supports IEEE 1609.2 and IEEE 1609.2.1 certificate handling requirements, including Enrollment Certificate provisioning, application certificate provisioning, and secure storage of associated private keys. The RSU constructs and validates certification paths using the active Certificate Trust List (CTL), enforces PSID and SSP authorization constraints, and verifies certificate revocation status using SCMS-defined Certificate Revocation Lists

(CRLs) or equivalent mechanisms before accepting signed messages. Private key access is restricted to authorized processes and protected within secure cryptographic modules or hardware-backed storage where supported.

For management-plane and backhaul communications, the IOO determines whether SCMS credentials or a separate X.509-based enterprise PKI is used. The manufacturer ensures the RSU supports standards-based certificate chain validation to trusted root authorities and enforces mutual authentication where required. When separate PKI domains are used for V2X and management communications, the manufacturer maintains logical and cryptographic separation of trust anchors and private key material. Where cross-domain trust is required, the IOO ensures the selected PKI providers define appropriate trust relationships consistent with NIST SP 800-57 Part 1.

Risk References and Resources:

ARC-IT Mechanisms: See control IA-05

ARC-IT Protocol Implementation Statements:

- Stores PKI-based credentials
- Supports X.509⁽³⁸⁾ certificate chain construction.

Standards: NIST SP 800-57 Part 1⁽²⁹⁾, IEEE 1609.2.1.⁽¹⁹⁾

IA-5(14), Authenticator Management | Managing Content of PKI Trust Stores

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 manages PKI trust relationships by selecting approved SCMS and enterprise PKI providers and ensuring RSUs are configured to trust only authorized root and intermediate certificate authorities. Trust anchor content, Certificate Trust Lists (CTLs), and Certificate Revocation Lists (CRLs) are obtained from the applicable PKI provider in accordance with the governing Certificate Policy.

The manufacturer ensures the RSU maintains protected trust stores for SCMS and, where applicable, enterprise PKI domains. The RSU validates the authenticity and integrity of CTLs, trust anchor updates, and CRLs before installation and applies updates in a manner that prevents partial or inconsistent trust states. The RSU rejects certificates chaining to untrusted, expired, or revoked trust anchors and enforces revocation checking prior to accepting authenticated connections or signed messages.

Trust store updates occur in response to PKI provider notifications, root rollover events, compromise declarations, or policy updates. The RSU prevents unauthorized modification of trust store content and logs trust store changes in accordance with audit requirements.

Standard: IEEE 1609.2.1.⁽¹⁹⁾

IA-7, Cryptographic Module Authentication

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Use of unsecure ITS protocols” in table 6, Communication and Network Configuration Vulnerabilities and Predisposing Conditions.

Guidance: RSUs rely on cryptographic modules to perform key generation, digital signature, encryption, and certificate validation operations required for V2X messaging and secure management communications. The manufacturer integrates a cryptographic module that meets applicable FIPS 140-3 validation requirements or equivalent approved validation where mandated by procurement policy. The module supports secure key generation, storage, and cryptographic processing consistent with IEEE 1609.2 and applicable PKI requirements.

The manufacturer ensures private keys associated with Enrollment Certificates, application certificates, device TLS credentials, and other sensitive cryptographic material are generated and stored within the validated cryptographic boundary and are not exportable in plaintext form. The module enforces role-based access controls so that only authorized processes and roles can invoke private key operations. Where operator authentication to the cryptographic module is required, the module enforces authentication mechanisms consistent with its validated security level.

The IOO defines procurement requirements for cryptographic module validation and verifies compliance during acquisition and deployment and ensures that deployed RSUs operate in accordance with the validation level required by organizational policy (e.g., FIPS 140-3 Levels 1-4).

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.

A 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 140-2 level 2.

Standard: FIPS 140-3⁽³⁴⁾

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: Non-organizational users include maintenance contractors, vendor support personnel, integrators, and other external parties who access the RSU for diagnostics, configuration, firmware updates, or incident response. The manufacturer designs the RSU to require unique identification and authentication for all non-organizational users prior to granting access to management interfaces, whether local or remote.

The IOO establishes policies governing contractor access, including account provisioning, authorization scope, session monitoring, and timely deactivation upon completion of work. Shared

accounts are avoided where feasible. If shared or emergency access mechanisms are required, the IOO defines compensating controls such as enhanced logging, limited time-bound credentials, physical supervision, or post-access review.

For remote contractor access, the manufacturer ensures the RSU enforces strong authentication mechanisms consistent with IA-2 requirements, including multifactor authentication where required by policy. Authentication exchanges occur only over cryptographically protected channels. The RSU logs contractor authentication events and administrative actions in accordance with applicable audit controls.

For local access in physically secured roadside cabinets, the IOO may rely on physical access controls as part of the authentication model where consistent with policy and risk tolerance.

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: RSUs authenticate V2X application services using SCMS-issued certificates in accordance with IEEE 1609.2 and IEEE 1609.2.1. Each V2X message is digitally signed using a valid application certificate that binds the signer to one or more Provider Service Identifiers (PSIDs) and associated Service Specific Permissions (SSPs). The manufacturer ensures the RSU enforces verification of PSID and SSP constraints during message validation so that only authorized services are permitted to transmit or be accepted.

For outbound messages, the RSU signs safety and infrastructure messages using application certificates provisioned under the applicable SCMS Certificate Policy. The RSU includes the appropriate PSID in the signed message and ensures the certificate authorizes that PSID and associated SSP constraints.

For inbound messages, the RSU validates the digital signature, constructs the certification path to a trusted root identified in the active Certificate Trust List (CTL), verifies certificate validity and expiration, checks revocation status using the applicable Certificate Revocation List (CRL), and confirms that the PSID and SSP values authorize the claimed service.

The IOO ensures the RSU is enrolled with an approved SCMS provider and operates under the applicable Certificate Policy.

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)

Standard: IEEE 1609.2.1.⁽¹⁹⁾

IA-11, Re-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: Re-authentication applies to user sessions established through RSU management interfaces. The IOO defines the conditions under which users must re-authenticate, including inactivity thresholds, privilege elevation, credential change events, or other risk-based triggers. The manufacturer implements RSU capabilities that enforce those conditions for local and remote management sessions.

The RSU enforces re-authentication after a defined period of session inactivity and upon expiration of an authenticated session token. The RSU also requires re-authentication prior to performing privileged operations if the existing session does not meet current authentication strength requirements. The IOO remains responsible for responding to organizational events such as role changes or account revocation, and the RSU enforces those changes once account status is updated through the applicable identity management mechanism.

Parameter Value(s):

“After 15 minutes of inactivity; upon session expiration; upon privilege elevation; and upon credential or account status 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 establishes and maintains an incident response training program for personnel responsible for RSU operations, maintenance, cybersecurity monitoring, and management. Training covers detection of anomalous V2X message behavior, certificate revocation events, CTL or CRL update failures, unauthorized configuration changes, failed authentication attempts, wireless interference, and backhaul communication disruptions.

The IOO ensures personnel understand reporting procedures, escalation paths, coordination with SCMS or PKI providers, evidence preservation requirements, and recovery procedures for roadside deployments. The training program includes participation in annual tabletop exercises that simulate

RSU-specific incident scenarios such as compromised certificates, firmware integrity failures, or loss of trusted SCMS connectivity. Lessons learned from these exercises are incorporated into updated procedures and role-specific training.

Training applies to operational staff, field technicians, security administrators, and incident response personnel who may interact with RSUs or supporting infrastructure.

Parameter Value(s):

paragraph a.1. “Annually and prior to granting access to RSU management functions.”

paragraph a.3. “Following significant system changes, SCMS policy updates, identified incident trends, or after-action findings from exercises.”

paragraph b. #1 “Annually, including participation in at least one tabletop exercise addressing RSU-related incident scenarios.”

Paragraph b #2 “Changes to system roles, responsibilities, threat environment, or incident response procedures.”

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 conducts incident response exercises that include RSU-specific scenarios such as compromised credentials, invalid or revoked V2X certificates, CTL rollover events, unauthorized firmware modification attempts, wireless interference, and loss of backhaul connectivity. Exercises validate detection capability, communication flow, containment procedures, and restoration of RSU operations without disrupting safety messaging beyond acceptable operational thresholds.

Testing may include tabletop exercises, simulated certificate revocation events, coordinated drills with SCMS providers, and recovery validation for field-deployed devices. The IOO ensures testing does not adversely affect live roadway safety operations and may use staging or simulated environments where appropriate.

Parameter Value(s):

“At least 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 establishes incident handling procedures that address preparation, detection, analysis, containment, eradication, recovery, and post-incident review for RSU-related events. Procedures include coordination with SCMS or PKI providers for certificate revocation or re-enrollment, validation of CTL or trust anchor updates following compromise, and restoration of known-good firmware or configuration baselines.

Risk References and Resources:

NIST SP 800-82: 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.

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 schedules, authorizes, documents, and reviews all RSU maintenance activities. Maintenance is performed in accordance with manufacturer specifications and organizational security procedures. When RSUs or components are removed for off-site repair, the IOO ensures sensitive configuration data, credentials, and audit logs are sanitized or removed prior to transfer.

Maintenance personnel verify that security configurations, firmware integrity, certificate status, and network settings are restored to an approved baseline following maintenance. The IOO maintains records of maintenance activities, including the identity of the technician, actions performed, and components serviced. Physical integrity of enclosures, fasteners, seals, and external hardware is also verified due to the exposed roadside environment.

Parameter Value(s):

paragraph c. “Authorized system administrators or designated maintenance personnel.”

paragraph d. “System security configurations, network configurations, device credentials and certificates, and audit log data.”

paragraph f. “Maintenance date and time; technician identity; components serviced; configuration or firmware changes performed.”

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 on RSUs, including diagnostic software, firmware update utilities, and configuration applications. Only authorized tools are permitted to interface with the RSU through local or remote management interfaces.

The manufacturer designs the RSU to restrict access to maintenance interfaces and to prevent unauthorized media or hardware devices from interfacing with physical ports where feasible. Maintenance sessions are authenticated and logged in accordance with identification and audit controls.

Parameter Value(s):

paragraph b. "Reviewed at least 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 implements a process for applying firmware and software updates to RSUs in a controlled manner. The manufacturer ensures the RSU verifies authenticity and integrity of updates using vendor cryptographic signatures prior to installation. Updates are tested in a staging or controlled environment where feasible and are applied in coordination with operational requirements to minimize disruption to V2X messaging. All update events are logged.

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 authorizes and monitors all nonlocal maintenance activities involving RSUs. Remote maintenance sessions require strong authentication consistent with IA-2 and IA-5 controls and are limited to approved maintenance windows or operational needs.

The manufacturer ensures the RSU supports secure remote maintenance sessions using encrypted channels and enforces session termination upon completion or inactivity.

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 manufacturer ensures the RSU logs all nonlocal maintenance sessions and related administrative actions.

Parameter Value(s):

"Session date and time; authenticated user or device identity; source network address; session duration; configuration changes; firmware upload attempts; system access attempts."

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: Remote maintenance sessions are authenticated using mutually authenticated encrypted channels. Maintenance traffic is logically separated from V2X communications and other operational traffic using network segmentation or equivalent isolation mechanisms.

Parameter Value(s):

paragraph a. “Mutual TLS 1.3 in accordance with ISO 21177 using IEEE Std. 1609.2 certificates or X.509 certificates, protected within a validated cryptographic module or hardware-backed secure storage.”

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 agreements to ensure timely repair or replacement of critical RSU components following failure. Maintenance response times reflect the operational importance of the affected device and its role in safety messaging.

Parameter Value(s):

#1 “RSU device, antennas, secure enclosures, and critical communication modules.”

#2 “Within 24 hours for safety-critical deployments, or as defined by operational impact assessment.”

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: RSUs are typically deployed in roadside cabinets or pole-mounted enclosures rather than traditional facilities. The IOO defines and manages physical access authorizations for those cabinets, including control of keys, access credentials, and role-based authorization for field personnel. The IOO maintains a list of individuals authorized to access RSU enclosures and reviews access authorizations periodically and upon personnel changes.

Parameter Value(s):

paragraph c. “At least annually and upon personnel transfer or termination.”

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 restricts physical access to RSU cabinets and associated roadside cabinet electronics to authorized roles such as installers, maintainers, and system administrators. Authorization is based on position or assigned role, and access is limited to individuals whose duties require direct interaction with the equipment.

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 implements physical controls to prevent unauthorized access to RSU cabinets and associated infrastructure. The manufacturer designs cabinets and enclosures to support locking mechanisms and controlled access. The IOO manages key distribution and ensures locks are replaced or rekeyed when access control is compromised or personnel changes occur.

Parameters Value(s):

paragraph a. “RSU cabinet enclosure, associated roadside cabinet electronics, traffic signal controller (TSC) interfaces within the cabinet, and exposed network or power cabling physically connected to the RSU.”

paragraph a.2. “Lockable enclosure using integrated keyed lock, restricted key system, electronic access control, or equivalent tamper-resistant locking mechanism.”

paragraph f. #2 “Access authorizations and key or access credential inventories are reviewed at least annually and immediately upon key loss, suspected compromise, or personnel transfer or termination.”

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: For RSU components installed in publicly accessible areas, the IOO enforces enhanced physical protections such as locked cabinets, restricted access panels, or elevated mounting locations to reduce unauthorized interaction.

Parameter Value(s):

paragraph a. "RSU cabinet and associated roadside cabinet electronics."

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 manufacturer designs RSU hardware and communication modules to reside within lockable enclosures. The IOO ensures enclosures remain secured and are inspected during maintenance activities.

Parameter Value(s):

"RSU communication modules and hardware components"

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 requires tamper resistance or tamper detection mechanisms for critical RSU components and cabinet enclosures. The manufacturer integrates appropriate tamper-evident seals, intrusion detection switches, or port disablement mechanisms to reduce risk of hardware manipulation.

Parameter Value(s):

#1 "Tamper-evident seals, cabinet intrusion detection switches, and disabling of unused external ports."

#2 "Prevent and detect unauthorized access."

#3 "Critical communication, cryptographic, and control components."

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, Physical Vulnerabilities and Predisposing Conditions.

Guidance: The IOO protects physical network and power cabling supporting RSUs using conduit, locked enclosures, or controlled routing to reduce tampering and accidental damage. The manufacturer supports secure interface placement within the cabinet design.

Parameter Value(s):

#1 "Network and power cabling supporting RSU operations."

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: The IOO implements monitoring mechanisms for RSU cabinet access where feasible, such as door-open sensors, tamper alerts, or integration with centralized monitoring systems. The manufacturer supports these capabilities within the cabinet or device design.

Parameter Value(s):

paragraph b.

#1 "at least annually"

#2 "Tamper alerts, unauthorized cabinet access, or detected physical intrusion events."

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 protects RSU power supplies, UPS units, and associated cabling from tampering or damage. The manufacturer designs internal cabling and power components to be protected within the enclosure.

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 RSUs require connection to backup or emergency power sources based on operational criticality. The manufacturer ensures the RSU can transition safely to an alternate power source without compromising configuration or cryptographic integrity.

Parameter Value(s):

"Transition of the system to emergency power"

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: The IOO defines environmental operating requirements for RSUs based on deployment conditions. The manufacturer designs cabinets and hardware to withstand defined temperature, humidity, and environmental exposure ranges consistent with applicable transportation equipment standards.

Parameters:

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-18, Location of System Components

Responsible Party (M/I): I

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

Guidance: The IOO selects RSU installation locations that reduce exposure to flooding, vandalism, accidental damage, or unauthorized access. Elevated mounting, locked cabinets, or pole-mounted installations are used where appropriate.

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 evaluates risk from electromagnetic interference, voltage spikes, or EMP-related events and defines protection requirements. The manufacturer designs shielding, surge protection, and grounding consistent with defined operational requirements.

Parameters:

#1 "Routine data backups", "Shielding"

#2 "Main controllers", "Data drives", "RSU communication modules and hardware components"

PL Family – Planning

PL-2 System Security and Privacy Plans

Responsible Party (M/I): M/I

Justification to Select: Threat “Inadequate organizational ownership of risk assessments” in table 3, Conduct an Attack (i.e., direct/coordinate attack tools or activities).

Guidance: The IOO develops and maintains a System Security Plan (SSP) that describes the RSU system boundary, system components, external interfaces, roles and responsibilities, and the security controls implemented to protect the system. The SSP identifies the types of data processed or transmitted by the RSU, the operational environment (roadside cabinet, TMC connectivity, wireless interfaces), management and maintenance access methods, interconnections with external systems (e.g., TMC, backhaul providers, certificate or credential services), applicable policies governing access control, logging, configuration management, incident response, and physical protection.

The SSP documents how selected security controls are implemented or inherited and assigns responsibility between the IOO and manufacturer where applicable. The plan is updated to reflect architectural changes, new interfaces, significant configuration changes, or security incidents.

Parameter Value(s):

paragraph a. “Security Administrator and System Owner responsible for maintaining the RSU System Security Plan.”

paragraph b. “Security Administrator, System Administrator, and other defined operational roles with responsibilities documented in the SSP.”

paragraph c. “At least annually and upon significant system, architectural, or operational changes.”

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): 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 develops and maintains a Concept of Operations (ConOps) that describes how RSUs are deployed, operated, monitored, maintained, and retired throughout their lifecycle. The ConOps explains the operational environment in which RSUs function, including roadside deployment conditions, connectivity to traffic management systems, use of wireless interfaces, and coordination with maintenance personnel and external service providers.

The document describes day-to-day operational workflows such as configuration management, software and firmware updates, remote and local maintenance activities, monitoring and alert handling, and escalation procedures. It also addresses how security considerations are integrated into routine operations, including access control practices, logging, incident handling coordination,

and protection of roadside equipment. The ConOps reflects the practical realities of field deployment and is updated when operational models, system architecture, or supporting services change.

Parameter Value(s):

paragraph b. “At least annually and upon major operational or architectural changes.”

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 5, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: The IOO maintains an inventory of deployed RSUs and associated critical components to support asset management, configuration management, vulnerability tracking, maintenance planning, and incident response. The inventory identifies each RSU by unique identifier and deployment location and records relevant hardware model information, firmware or software version, and operational status.

The inventory is used to track lifecycle events such as installation, replacement, upgrade, repair, and decommissioning. Manufacturers provide sufficient identifying and version information to allow accurate tracking of delivered components. The IOO updates the inventory as system changes occur and reconciles it periodically to ensure accuracy.

Parameter Value(s):

“Inventory reviewed and reconciled at least quarterly and updated upon installation, replacement, upgrade, or decommissioning of RSUs.”

RA Family – Risk Assessment

RA-3, Risk Assessment

Responsible Party (M/I): M/I

Justification to Select: Threat “Inadequate organizational ownership of risk assessments” in table 3, Conduct an Attack (i.e., direct/coordinate attack tools or activities).

Guidance:

The IOO conducts risk assessments for RSU deployments to identify threats, vulnerabilities, likelihood, and potential impacts to safety, operational continuity, data integrity, and public trust.

Assessments consider the physical exposure of RSUs in publicly accessible locations, wireless communications, remote management access, software and firmware integrity, and dependencies necessary for normal operation.

During design and development, the manufacturer performs product-level risk analysis and incorporates appropriate mitigations into the RSU architecture. The IOO reviews relevant security documentation and assurances provided by the manufacturer as part of acquisition and deployment planning. After deployment, the IOO assumes responsibility for ongoing risk assessment of the deployed RSU environment and coordinates with the manufacturer when product updates or technical mitigations are required.

Parameter Value(s):

paragraph d “At least annually and upon significant changes to system configuration, threat landscape, or deployment conditions.”

paragraph f. “At least annually or upon identification of significant new threats, vulnerabilities, or incidents affecting RSUs.”

Standard: NIST SP 800-30⁶

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

Responsible Party (M/I): M/I

Justification to Select: Threat “Inadequate organizational ownership of risk assessments” in table 3, Conduct an Attack (i.e., direct/coordinate attack tools or activities).

Guidance: The IOO assesses supply chain risks associated with RSU components, including hardware, firmware, software, and embedded third-party modules. The assessment considers supplier trustworthiness, component provenance, update mechanisms, and potential tampering risks during manufacturing, transport, and storage.

Manufacturers conduct internal supply chain risk management consistent with recognized standards and provide relevant assurance information during procurement. The IOO evaluates supplier risk posture when selecting vendors and incorporates supply chain considerations into acquisition and lifecycle planning.

Parameter Value(s):

paragraph a “Hardware, firmware, software, and third-party components determined to be critical to RSU functionality or security.”

paragraph b. “At least annually and prior to major procurement or supplier change.”

Standard: NIST SP 800-161⁽²⁶⁾

⁶ <https://csrc.nist.gov/pubs/sp/800/30/r1/final>

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: The IOO establishes a vulnerability management process appropriate for RSUs and their operational constraints. During development, the manufacturer performs vulnerability identification activities such as static analysis, dependency analysis, configuration review, and controlled scanning in test environments.

After deployment, the IOO monitors for vulnerabilities affecting RSU hardware, firmware, operating systems, and supporting services. Because RSUs may be sensitive to active scanning, the IOO selects scanning approaches based on risk, which may include passive monitoring, review of vendor advisories, comparison against public vulnerability databases, and testing in non-production or replicated environments. Active scanning of production RSUs is only scheduled during planned outages or avoided when operational impact is unacceptable.

Parameter Value(s):

paragraph a. “at least annually”

Risk References and Resources:

ATT&CK for ICS Mitigations / Techniques:

- M0916 / T0819

NIST SP 800-82: 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., Cybersecurity & Infrastructure Security Agency [CISA] advisories, NIST National Vulnerability Database [NVD]). 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 shall 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 shall 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 shall 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 Open Web Application Security Project [OWASP]-Top 10 vulnerabilities).
- Any Web applications (inaccessible from the public Internet) shall undergo a privileged access scan per [Control Enhancement 5] to identify issues affecting authenticated users.
- Application source code shall 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 shall be conducted.
- Application binaries shall 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 shall 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 of vulnerability assessment activities to include RSUs and supporting components whose compromise could materially affect safety, signal operations, or communications integrity. This may include the RSU device, embedded V2X modules, management interfaces, cabinet networking components, and associated field equipment where connected.

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: After identifying risks through assessment, monitoring, or scanning activities, the IOO selects and documents an appropriate risk response, which may include mitigation, transfer,

acceptance, or avoidance. Selected responses are prioritized based on potential safety impact, operational disruption, exploitability, and regulatory obligations.

Where mitigation requires product updates, configuration changes, or architectural modifications, the IOO coordinates with the manufacturer to implement appropriate corrective actions. Compensating controls may be applied when immediate remediation is not feasible.

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 cybersecurity requirements for RSUs as part of the acquisition process and incorporates those requirements into procurement documentation, contracts, and acceptance criteria. These requirements may address secure configuration defaults, authentication mechanisms, cryptographic capabilities, logging, maintenance access controls, and lifecycle support.

The manufacturer implements the required capabilities during design and development and provides sufficient evidence to demonstrate conformance with the acquisition requirements. The IOO determines the level of assurance required based on risk tolerance and operational impact. Where appropriate, the IOO may select additional control enhancements to increase design assurance or validation rigor.

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 provides example cybersecurity procurement language for ITS.

SA-4(2), Acquisition Process | Design and Implementation Information for Controls

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 requires the manufacturer to provide design and implementation information sufficient to evaluate the security of the RSU. This includes documentation of security-relevant interfaces, authentication mechanisms, cryptographic module boundaries, software and firmware update mechanisms, and management interfaces. Depending on risk and contractual agreements, the IOO may require additional detail such as high-level and low-level design documentation, interface specifications, or limited source code review.

Parameter Value(s):

#1. “Security-relevant external interfaces; high-level and low-level design documentation; cryptographic module boundary descriptions; protocol specifications; and, where contractually required, source code or hardware design information.”

#3. “Documentation at the module level, including identification of cryptographic boundaries and protocol implementations.”

Risk References and Resources:

NIST SP 800-82:⁽³⁾ When acquiring ITS products, consideration for security requirements may not have been incorporated into the design. Procurement may need to consider alternative products or complementary hardware, or plan for compensating controls.

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 defines required secure configuration baselines for RSUs as part of acquisition. The manufacturer delivers RSUs configured to meet those baseline requirements by default or provides documented procedures to achieve the required configuration prior to deployment.

Secure configuration expectations may include disabling unused ports and services, enforcing authentication prior to management access, enabling secure transport protocols such as TLS 1.3 where supported, disabling insecure legacy protocols, and enforcing least functionality. Wireless interfaces are configured to operate only as required for mission needs.

Parameter Value(s):

paragraph a. “Organization-defined secure configuration baseline, including approved functions, ports, protocols (with version requirements), services, and cryptographic settings.”

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 specifies, as part of acquisition, the functions, ports, protocols, and services that the RSU is required to support and those that must be disabled or restricted. Version requirements for protocols are defined where applicable. The manufacturer ensures the RSU supports configuration controls that allow enforcement of these requirements and prevents unauthorized enablement of additional 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: The manufacturer provides system documentation for the RSU and any integrated applications sufficient to support secure installation, configuration, operation, maintenance, and troubleshooting. Documentation includes security-relevant configuration settings, authentication mechanisms, logging capabilities, update procedures, and interface descriptions.

The IOO ensures that documentation necessary for secure deployment and ongoing administration is retained and made available to authorized personnel. Documentation is updated when firmware, software, or supported configurations materially change.

Parameter Value(s):

paragraph d. "System owner, system security officer, system administrator, and other authorized operational or maintenance roles as defined by the IOO."

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 recognized security and privacy engineering principles into acquisition requirements and system design expectations for RSUs. The manufacturer applies these principles during architecture, design, and implementation of hardware, firmware, and software components.

Security considerations are integrated throughout the development lifecycle rather than added after deployment. Design practices address least functionality, secure configuration defaults, strong authentication, protection of cryptographic material, separation of management and operational interfaces, and resilience to misuse or fault conditions.

Parameter Value(s):

"Least privilege, secure defaults, defense in depth, fail securely, complete mediation, separation of duties, minimized attack surface, 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: This control applies when RSUs rely on external system services, such as managed backhaul providers, certificate or credential management services, cloud-hosted management platforms, or remote monitoring systems.

The IOO defines security requirements for those services, including authentication, encryption, logging, availability expectations, and incident reporting obligations. The IOO ensures that service agreements document security responsibilities, data handling requirements, and coordination procedures for security events.

Parameter Value(s):

paragraph a. "Organization-defined security requirements for external services, including authentication, encryption, logging, availability, and incident reporting obligations."

paragraph c. "Periodic review of external service security posture at least annually and upon significant service or contractual change."

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 the functions, ports, protocols, and services required for interaction with external system services and ensures that only those necessary for mission operations are enabled. Requirements are defined during acquisition and reflected in configuration baselines. Unused or unsupported services are disabled.

Parameter Value(s):

“Organization-defined approved external interfaces, ports, protocols (with version requirements), and services required for interaction with external system services.”

SA-10, Developer Configuration Management

Responsible Party (M/I): M

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 formal configuration management processes during the design, development, integration, testing, release, and maintenance of RSU hardware, firmware, and software. Configuration items are uniquely identified, version controlled, and subject to documented change control procedures. Changes are reviewed, approved, tested, and traceable to requirements, defect reports, or security findings.

Parameter Value(s):

paragraph a. “Design, development, integration, testing, release, and maintenance phases.”

paragraph b. “All hardware design artifacts, firmware, software source code, build configurations, third-party libraries, and security-relevant configuration files.”

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

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 protects the integrity of RSU software and firmware throughout development and release. Official release images are uniquely versioned and cryptographically signed prior to distribution. Build processes are controlled to prevent unauthorized modification of source code, build scripts, or compiled artifacts.

The RSU validates the authenticity and integrity of firmware and software updates before installation using approved digital signature verification mechanisms. Only manufacturer-authorized and properly signed updates are accepted by the device.

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 controls during production and assembly of RSUs. These controls include component traceability, controlled manufacturing processes, inspection and validation procedures, and protection against unauthorized modification of hardware components.

Where supported by the design, the RSU uses hardware-rooted mechanisms, such as secure boot anchored in immutable hardware or verification of trusted hardware components at startup, to ensure that only authorized firmware executes on the device.

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 performs security testing and evaluation activities throughout the RSU development lifecycle. Security testing is integrated into unit, integration, system, and regression testing processes and is performed prior to release of production firmware or software. Testing verifies correct implementation of authentication mechanisms, cryptographic operations, access controls, input validation, logging, and update mechanisms.

Security defects identified during testing are documented, tracked, and resolved prior to release or formally accepted under the manufacturer's secure development policy. Testing results are retained to support traceability between identified vulnerabilities and remediation actions.

Parameter Value(s):

paragraph b. #1 "Unit, integration, system, regression, and security-focused test activities."

paragraph b. #2 "At each major release and for security-relevant changes."

paragraph b. #3 "Full security test coverage for authentication, cryptographic, and update mechanisms; risk-based coverage for other 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. Analyses consider the RSU's functional architecture, externally reachable interfaces, wireless communications, management interfaces, and protection of cryptographic material.

Threat modeling addresses both system-level risks and component-level vulnerabilities, particularly those affecting authentication, authorization, cryptographic key protection, message integrity, firmware integrity, and privilege boundaries. The manufacturer uses recognized methodologies and maintains documentation of identified threats, mitigations, and residual risks.

Parameter Value(s):

paragraph a. "System architecture, externally reachable interfaces, wireless and management interfaces, cryptographic components, and known threat patterns."

paragraph b. "Threat modeling, static code analysis, dynamic testing, dependency analysis, vulnerability scanning, and penetration testing in controlled environments."

paragraph c. "System-level threat analysis and detailed component-level analysis for authentication, authorization, cryptographic, and update mechanisms."

paragraph d. "Threat model reviewed and approved by qualified security engineering personnel; high-severity vulnerabilities remediated or formally accepted under documented policy."

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

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 conducts attack surface reviews throughout development to identify externally reachable services, enabled ports and protocols, wireless interfaces, update mechanisms, debugging interfaces, and third-party components. Reviews verify that only required functionality is exposed and that security controls such as authentication, input validation, encryption, and rate limiting are consistently applied. Attack surface documentation is updated with each major firmware or architectural revision and maintained under developer configuration management.

SA-17, Developer Security and Privacy Architecture and Design

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 defines and documents the RSU’s security architecture during system design. The architecture identifies trust boundaries, privilege separation mechanisms, cryptographic module boundaries, secure boot processes, firmware update validation mechanisms, and protection of sensitive data. Security architecture documentation demonstrates how layered protections, least privilege, secure defaults, and isolation between management and operational functions are implemented. Where the RSU processes operational data that could implicate privacy considerations, data minimization and controlled retention principles are incorporated into design decisions.

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 manufacturer defines support lifecycles for RSU hardware, firmware, software, and embedded third-party components and communicates end-of-support timelines. The manufacturer provides patches, updates, or upgrade paths during the supported lifecycle.

The IOO tracks deployed RSU versions and plans for replacement, upgrade, or compensating controls when components approach or reach end of support. Continued operation of unsupported components is formally evaluated for risk and documented.

Parameter Value(s):

paragraph b. “In-house support or support from organization-approved external providers when vendor support is no longer available.”

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 RSU to logically separate system management functionality from operational functionality. Administrative interfaces, operating system management functions, configuration services, firmware update mechanisms, and security settings are accessible only to authenticated and authorized privileged roles.

Operational functions, such as V2X message transmission and interaction with signal or field interfaces, execute in restricted contexts that do not permit modification of system-level configuration or access to underlying operating system services.

Development and debugging functionality is removed, disabled, or cryptographically restricted in production builds. Any retained diagnostic interfaces are protected by strong authentication and are not accessible through non-privileged operational interfaces.

Logical separation is enforced through role-based access control, process isolation, and privilege boundaries within the operating system and application architecture.

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 ensures that non-privileged interfaces do not provide access to system-level administration or security functions. Non-privileged roles are prevented from accessing operating system shells, modifying configuration files, changing security settings, installing software, updating firmware, modifying certificate stores, or altering logging behavior.

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 designs the RSU so that security functions are logically and, where feasible, hardware-enforced isolated from non-security functions. Security functions include cryptographic operations, private key handling, certificate validation, authentication processing, secure boot verification, and access control enforcement.

Isolation mechanisms may include processor privilege levels, memory protection mechanisms, secure execution environments, hardware security modules, or other hardware-backed protections. Security-relevant code and data are protected through address space separation, file system permissions, and restricted inter-process communication. Non-security applications cannot directly access private keys, cryptographic material, or security configuration data.

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: The manufacturer implements hardware-enforced mechanisms to isolate critical security functions from general system processes. This may include hardware-rooted secure boot, memory protection units, trusted execution environments, or dedicated cryptographic modules.

Cryptographic key storage and sensitive security operations are executed within protected hardware or hardware-backed environments that prevent unauthorized read, modification, or extraction of private keys and other sensitive security data.

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: The manufacturer ensures that access control enforcement and security decision functions are isolated from application logic and diagnostic or monitoring components. Authentication processing, authorization checks, certificate validation, and policy enforcement mechanisms are implemented in controlled execution contexts that cannot be modified or bypassed by non-security processes.

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 minimizes non-security functionality within privileged or security-sensitive execution contexts. Security modules are designed to perform only their defined security functions and do not include unrelated application logic, diagnostic utilities, or user-accessible services. This reduces complexity and limits the potential attack surface within security-critical components.

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 IOO defines availability objectives for RSUs and identifies the types of denial-of-service conditions that could materially impact safety or operational continuity. These may include network flooding, excessive management-plane requests, malformed or excessive application-layer messages, radio frequency interference, or resource exhaustion affecting CPU, memory, or storage.

The manufacturer designs the RSU to incorporate protective mechanisms appropriate to its role and resource constraints. These mechanisms may include rate limiting on management interfaces, prioritization of safety-critical processing over non-critical services, validation and rejection of malformed messages, resource threshold protections, and protective filtering at network interfaces.

Where protection cannot be fully implemented at the RSU due to hardware or performance constraints, the IOO implements complementary controls in upstream network devices or infrastructure.

Parameter Value(s):

paragraph a. #1 “Protect”

#2 “Network flooding, excessive management requests, malformed or excessive V2X messages, radio frequency interference, and resource exhaustion conditions.”

paragraph b. “Rate limiting on management interfaces; prioritization of safety-critical processing; validation and rejection of malformed traffic; resource threshold protection; and stateful network filtering where supported.”

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 the RSU cannot be readily used as a platform to launch denial-of-service attacks against other systems. The RSU limits outbound traffic to defined operational functions and does not allow arbitrary packet generation or unrestricted forwarding.

The RSU restricts broadcast, multicast, and management-plane traffic to only those functions necessary for operation. It prevents spoofed source address transmission where applicable and enforces protocol constraints consistent with its intended use.

Parameter Value(s):

“Outbound traffic restricted to organization-defined operational protocols and services; prevention of unauthorized packet forwarding or arbitrary traffic generation.”

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 RSU with sufficient processing capacity and network interface capability to handle expected peak loads of legitimate traffic, including V2X message volumes and management communications. Resource allocation mechanisms prioritize critical functions to prevent starvation by lower-priority processes.

Where appropriate, upstream infrastructure devices such as routers or firewalls provide additional bandwidth management, traffic shaping, or redundancy to support availability objectives.

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 monitoring expectations for detecting potential denial-of-service conditions affecting RSUs. The manufacturer implements logging and telemetry capabilities that allow detection of abnormal traffic rates, repeated authentication failures, message validation failures, resource exhaustion events, or radio anomalies.

The RSU generates logs or alerts when resource thresholds are exceeded or when abnormal traffic patterns are detected. Aggregated monitoring and correlation are typically performed at centralized management or traffic management systems rather than directly on the RSU.

Parameter Value(s):

paragraph a. “Abnormal traffic rate detection; repeated authentication failures; malformed message rates; resource utilization thresholds; and radio interference indicators.”

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 RSU to manage and control consumption of critical system resources to ensure continued availability of safety and management functions. The RSU implements mechanisms to prevent any single process, interface, or service from exhausting processing capacity, memory, storage, or network bandwidth.

Critical functions, such as V2X message processing, certificate validation, and authenticated management access, are prioritized over non-critical services. Resource controls may include scheduling priorities, memory protections, connection limits, rate limiting, and quotas for management-plane services. When resource thresholds are approached, the RSU maintains operation of defined essential functions and degrades non-essential functionality in a controlled manner.

Parameter Value(s):

#1 “CPU utilization, memory allocation, storage capacity, network bandwidth, and connection/session limits.”

#2 “Process prioritization, resource quotas, rate limiting, and connection limits for non-critical services.”

SC-7, Boundary Protection

Responsible Party (M/I): M

Justification to Select: Vulnerability “Firewalls nonexistent or improperly configured” in table 6, Communication and Network Configuration Vulnerabilities and Predisposing Conditions.

RSUs operate at the edge of transportation networks and communicate over wireless, wired backhaul, and management interfaces. Without clearly defined and enforced communication boundaries, unauthorized traffic could reach management interfaces, cryptographic services, or other sensitive functions. Boundary protection is necessary to restrict communications to authorized peers, protocols, and interfaces and to reduce exposure of the RSU attack surface.

Guidance: The manufacturer designs the RSU to enforce logical boundary protections at all network-facing interfaces. The RSU restricts inbound and outbound communications to organization-defined protocols, ports, and peer systems. Filtering may include packet inspection, stateful connection tracking, protocol validation, and enforcement of allow-listed communication paths.

Boundary protection applies to management interfaces, backhaul connectivity, and any other routable interfaces. The RSU does not expose unnecessary services and does not rely solely on upstream network devices for protection. Communication policies are configurable so the IOO can define authorized peers and services.

Parameter Value(s):

paragraph b. "Logically enforced at each routable network interface.

"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): M/I

Justification to Select: Vulnerability "No security perimeter defined" in table 6, Architecture and Design Vulnerabilities and Predisposing Conditions.

Guidance: The IOO defines approved external access points into the ITS network that may communicate with RSUs, such as managed gateways or VPN termination points. The manufacturer ensures the RSU supports configuration of trusted ingress points and does not permit arbitrary external access.

RSUs do not independently establish unmanaged external access paths. Remote maintenance access is routed through defined and controlled access points consistent with organizational policy.

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

Justification to Select: Vulnerability "Inadequate security policy for ITS" in table 6, Policy and Procedure Vulnerabilities and Predisposing Conditions.

Guidance: The manufacturer implements a deny-by-default communication policy at RSU network interfaces. Only explicitly authorized protocols, ports, and peer addresses or authenticated identities are permitted. All other traffic is rejected.

Allow-lists may be based on IP addresses, authenticated device identities, certificates, or other organization-defined criteria.

Parameter Value(s):

"At managed network interfaces for RSUs and associated backhaul connections."

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: Where remote devices establish VPN connections to access RSUs or supporting systems, the IOO defines whether split tunneling is permitted. If prohibited, VPN configurations enforce routing of all traffic through approved gateways. The RSU does not independently manage split tunneling policies but supports secure VPN-based access where applicable.

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, Section Architecture and Design Vulnerabilities and Predisposing Conditions.

Guidance: The manufacturer minimizes and protects physical communication interfaces such as UART, SPI, USB, Ethernet, or other debug ports. Unused ports are disabled, removed, or cryptographically restricted in production units. Where ports remain accessible, they require strong authentication or are protected within locked enclosures.

The IOO enforces physical protections such as locked cabinets and tamper detection consistent with physical security controls.

Parameter Value(s):

“Debug and maintenance interfaces including UART, SPI, USB, and Ethernet ports.

”Standard: IEEE 802.1X⁽⁴²⁾ & 802.3⁽⁴³⁾

SC-7(16), Boundary Protection | Split Tunneling for Remote Devices

Responsible Party (M/I): M

Justification to Select: Vulnerability “Perform perimeter network reconnaissance/scanning” in table 6, Perform Reconnaissance and Gather Information.

Guidance: The manufacturer ensures that the RSU does not advertise unnecessary network services and does not expose management interfaces beyond defined boundary protections. Network discovery services not required for operation are disabled.

SC-7(18), Boundary Protection | Fail Secure

Responsible Party (M/I): M

Justification to Select: Threat event “Loss of Safety” in table 4, and vulnerability “Firewalls nonexistent or improperly configured” in table 6, Communication and Network Configuration Vulnerabilities and Predisposing Conditions.

Guidance: The manufacturer designs boundary protection mechanisms so that failures default to a secure state. If filtering or enforcement components fail, unauthorized traffic is not permitted by default. Upon power restoration or restart, boundary protections are restored before non-essential services resume.

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 RSU supports configuration of approved peer systems or authenticated device identities for management and backhaul communications. Communications from non-approved or unauthenticated hosts are rejected.

Parameter Value(s):

“Organization-defined trusted peer systems or authenticated device identities.”

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 and implements logical isolation of RSUs within the ITS network architecture. RSUs are deployed within dedicated or appropriately segmented network zones separate from non-critical or unrelated field devices. Segmentation may be implemented using VLANs, VRFs, private APNs, firewalls, or other network boundary technologies.

Parameter Value(s):

#1. Roadside Units and V2X radio modules

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 restricts direct connections between RSUs and public networks. Where connectivity over public infrastructure is required, communications are established through managed gateways, private network services, or encrypted tunnels consistent with organizational security policy. Direct, unmanaged public exposure of RSUs is prohibited.

Parameters:

“Roadside Units (RSUs), including their management interfaces, V2X radio modules, and backhaul network interfaces.”

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.

RSUs communicate over wireless and wired networks that extend beyond physically controlled boundaries. These communications are subject to interception, modification, replay, or spoofing. Protection of transmission integrity is critical to prevent manipulation of safety-related messages, while confidentiality is required for management, credentialing, and operational communications.

Guidance: The manufacturer implements cryptographic mechanisms to protect data transmitted by the RSU over untrusted or externally accessible networks.

For management and backhaul communications, the RSU implements mutually authenticated TLS sessions using approved cryptographic algorithms consistent with RFC 8446 (TLS 1.3) or organizationally approved equivalents. Communications with TMCs, back-office systems, or maintenance devices are encrypted and integrity-protected.

For V2X safety messaging, the RSU implements IEEE 1609.2 message security services. Outbound messages are digitally signed using valid SCMS-issued certificates. Inbound messages are verified by validating digital signatures and certificate chains to trusted SCMS roots. Integrity and authenticity are mandatory; confidentiality is applied only where defined by the applicable V2X standard or service.

Cryptographic mechanisms are implemented using validated cryptographic modules where required by policy. Integrity protection is prioritized for safety messaging, as message manipulation presents higher operational risk than disclosure of most broadcast data elements.

Parameter Value(s):

“Mutually authenticated TLS 1.3 for management and backhaul communications; IEEE 1609.2 digital signature verification and generation for V2X message security.

”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

Standard: RFC 8446 Internet Engineering Task Force (IETF), The TLS Protocol Version 1.3, August 2018.⁽²¹⁾

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: The manufacturer implements cryptographic protections for all RSU communications traversing untrusted networks. TLS sessions use approved cipher suites and enforce certificate validation. V2X message security uses digital signature algorithms and certificate validation consistent with IEEE 1609.2 and applicable SCMS requirements.

Cryptographic operations are performed using modules validated under FIPS 140-3 where required by organizational policy.

Parameter Value(s):

“detect changes to information”

“FIPS 140-3 validated cryptographic modules; TLS 1.3 with organization-approved cipher suites; IEEE 1609.2 compliant digital signature algorithms.”

Standards: FIPS 140-3,⁽³⁴⁾ RFC 8446⁽²¹⁾

SC-8(2), Transmission Confidentiality and Integrity | Pre- and Post-Transmission Handling

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 manufacturer ensures that data is cryptographically protected prior to transmission and validated upon receipt. For management and backhaul traffic, encryption and integrity protections are applied within the TLS session before data leaves the device. For V2X messaging, messages are digitally signed prior to broadcast and validated upon receipt using signature verification and certificate chain validation.

Parameter Value(s):

"confidentiality and integrity"

Standards: FIPS 140-3,⁽³⁴⁾ FIPS 197,⁽³⁵⁾ RFC 8446⁽²¹⁾

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).

Authentication and configuration functions on RSUs are sensitive operations. Without a trusted path, an attacker could intercept credentials, spoof management interfaces, or manipulate security-relevant configuration actions. A trusted path ensures that authorized users interact directly with RSU security functions over an authenticated and integrity-protected channel.

Guidance: The manufacturer designs the RSU to provide a trusted communication path between users and defined security functions. Trusted paths are logically isolated and cryptographically protected to prevent interception or spoofing. For remote access, trusted paths are implemented through mutually authenticated secure sessions. For local access, trusted paths are implemented through authenticated console interfaces or equivalent secure mechanisms.

The trusted path is used for authentication, credential management, and security configuration functions.

Parameter Value(s):

“Authentication, credential management, and security configuration functions.”

SC-12, Cryptographic Key Establishment and Management

Responsible Party (M/I): M/I

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).

RSUs rely on cryptographic mechanisms for management communications and V2X message authentication. Weak key generation, storage, distribution, or destruction could allow impersonation, message forgery, or compromise of trust anchors. Proper key establishment and lifecycle management are essential to maintain trust in both SCMS-based V2X operations and management/backhaul communications.

Guidance: The IOO defines applicable key management requirements by contracting with an SCMS provider for V2X credentialing and, where applicable, with an enterprise PKI provider for management and backhaul communications. The manufacturer designs the RSU to support those key management requirements.

For V2X operations, the RSU supports secure enrollment, certificate provisioning, and key lifecycle processes consistent with IEEE 1609.2 and the applicable SCMS Certificate Policy and Enrollment Requirements. Private keys associated with Enrollment Certificates and application certificates are generated and stored within secure cryptographic modules and are not exportable in plaintext.

For management and backhaul communications, the RSU supports establishment and management of X.509-based device credentials consistent with the applicable PKI policy. The RSU enforces certificate validation, renewal, and revocation in accordance with the issuing authority’s policies.

Key generation, storage, rollover, revocation, and destruction processes align with applicable NIST guidance, including NIST SP 800-56A and NIST SP 800-57 Part 1, as required by organizational policy.

Parameter Value(s):

“In accordance with applicable SCMS Certificate Policy and Enrollment Requirements, IEEE 1609.2, and organization-approved PKI policies consistent with NIST SP 800-57 Part 1.

Standard: NIST SP 800-56A Rev. 3⁽²⁴⁾

SC-12(3), Cryptographic Key Establishment and Management | Asymmetric Keys

Responsible Party (M/I): M/I

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 IOO defines approved asymmetric cryptographic mechanisms for RSU operations through its contracted SCMS and enterprise PKI providers. The manufacturer ensures the RSU supports those mechanisms for V2X message authentication and management communications.

For V2X messaging, asymmetric keys and certificates conform to IEEE 1609.2 and associated SCMS requirements. For management and backhaul communications, asymmetric keys conform to organization-approved X.509-based PKI policies.

Private keys are generated and stored within secure cryptographic modules and are protected against unauthorized extraction or modification.

Parameter Value(s):

“IEEE 1609.2-compliant asymmetric cryptographic mechanisms for V2X operations and organization-approved X.509-based PKI mechanisms for management and backhaul communications using NIST-approved algorithms.

Standard: NIST SP 800-57 Part 1⁽²⁹⁾

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 manufacturer implements cryptographic protections for RSU communications and security-relevant functions in accordance with applicable standards and organizational policy.

For V2X operations, the RSU implements cryptographic protections defined in IEEE 1609.2 to provide message authentication and integrity for broadcast safety messages. Confidentiality is applied only where defined by the applicable V2X service.

For management and backhaul communications, the RSU implements cryptographic protections using mutually authenticated secure transport sessions. The RSU validates peer certificates and enforces integrity and confidentiality protections consistent with organizational PKI policy.

Cryptographic mechanisms are implemented using approved algorithms and validated modules where required by policy.

Secure boot and firmware integrity mechanisms use cryptographic validation to ensure only authorized software executes on the RSU.

Parameter Value(s):

“Digital signature–based integrity protection for V2X safety messages in accordance with IEEE 1609.2; mutually authenticated TLS for management and backhaul communications; cryptographic verification of firmware and software updates; and approved random number generation for key material.”⁽¹⁷⁾

Risk References and Resources:

ARC-IT Mechanisms:

- Devices may support additional cryptographic algorithms.
- Devices shall provide a FIPS 140-3 compliant random number generator, i.e., compliant to NIST SP 800-90A Revision 1.⁷

⁷ National Institute of Standards and Technology, Gaithersburg, MD, NIST Special Publication (SP) 800-90A Revision 1, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, June 2015.

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 and “Obtain sensitive information through network sniffing of external networks”, Section Achieve results (i.e., cause adverse impacts, obtain information). Create Attack Tools.

RSUs rely on public key certificates for V2X message authentication and for secure management communications. Improper issuance, validation, or trust anchor management could enable certificate spoofing, impersonation, or acceptance of counterfeit credentials. Public key certificates must be issued and managed under approved certificate policies and trusted infrastructures.

Guidance: The IOO contracts with an approved SCMS provider for issuance and lifecycle management of IEEE 1609.2-compliant certificates. The RSU must meet the applicable SCMS enrollment and end-entity security requirements prior to receiving credentials.

The manufacturer designs the RSU to support secure key generation, certificate enrollment, certificate installation, renewal, revocation processing, and trust store management in accordance with the applicable SCMS Certificate Policy and Certification Practice Statement.

The RSU supports secure enrollment processes with the SCMS Enrollment Authority, including mutual authentication and protected transport during credential provisioning. Private keys associated with Enrollment Certificates and application certificates are generated and stored within secure cryptographic modules and are not exportable in plaintext.

The IOO ensures the RSU maintains an updated Certificate Trust List (CTL) and applicable trust anchors required for validating V2X message certificates. The RSU processes Certificate Revocation Lists (CRLs) and other SCMS-defined revocation artifacts in accordance with policy.

For management and backhaul communications, the IOO obtains device certificates from an approved enterprise PKI service provider or issues certificates under an approved X.509-based certificate policy. The manufacturer ensures the RSU supports certificate validation and trust store separation between SCMS-based V2X operations and management-plane PKI operations.

The RSU maintains secure connectivity required to perform certificate renewal, revocation checking, and trust store updates as defined by the applicable certificate policy.

Parameter Value(s):

paragraph a “IEEE 1609.2-compliant certificates issued under an approved SCMS Certificate Policy and Certification Practice Statement, and X.509 certificates issued under an organization-approved PKI policy for management and backhaul communications.”

Standards: X.509⁽³⁸⁾ or IEEE STD.1609.2⁽¹⁶⁾

SC-24, Fail in Known State

Responsible Party (M/I): M

Justification to Select:

RSUs operate in distributed roadside environments where power disruptions, hardware faults, or cyber events may occur. If an RSU fails unpredictably, it could transmit malformed or unauthenticated messages, expose management interfaces, or corrupt configuration data. Failing in a defined and controlled state limits security and operational risk.

Guidance: The manufacturer designs the RSU to transition to a defined and controlled state upon detection of system faults, power interruptions, software crashes, or integrity violations.

The failure state prevents unauthorized access, prevents transmission of unauthenticated or malformed V2X messages, and preserves the integrity of stored configuration and credential data. Upon restart, the RSU verifies firmware integrity and restores cryptographic and boundary protections before resuming normal operations.

Parameter Value(s):

#1: "Block unauthorized communications; cease transmission of unsigned or unverified V2X messages; restrict management access to authenticated sessions only."

#2: "Power interruption or brownout; cryptographic module failure; certificate validation failure; firmware integrity verification failure; operating system crash; detected security compromise."

#3: "RSU configuration settings; cryptographic keys and certificates; certificate trust lists (CTLs) and trust anchors; audit log data; firmware integrity 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: RSUs are deployed in publicly accessible roadside environments and may be subject to physical access or hardware tampering. Stored configuration data, cryptographic credentials, and audit records must be protected to prevent unauthorized modification or disclosure.

Guidance: The manufacturer implements mechanisms to protect defined information stored on the RSU from unauthorized disclosure and modification.

Integrity protection is required for configuration files, certificate trust lists, revocation artifacts, firmware images, and audit logs to ensure stored data is not altered without detection.

Confidentiality protection is required for sensitive cryptographic material and any management credentials stored on the device.

Parameter Value(s):

#1 "Confidentiality & Integrity",

#2 "Confidentiality and integrity protection for RSU cryptographic keys, device certificates, configuration data, certificate trust lists (CTLs), certificate revocation lists (CRLs), firmware images, and audit logs."

Risk References and Resources:

ATT&CK for ICS Mitigations / Techniques:

- M0941 / T0839, T0857

ARC-IT Mechanisms:

- The device shall encrypt data on disk if that data is accessed only by entities with periodic privileged access as defined in Notes on Access Control⁸.
- 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 shall 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.

Standard: FIPS 140-3⁽³⁴⁾, FIPS 197⁽³⁵⁾

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: The RSU must implement mechanisms to preserve the integrity of data at rest, as outlined in NTCIP 1218 Section 3.6.1.2.1.,⁽⁴⁷⁾ which mandates verification of data integrity during storage. The manufacturer/vendor is responsible for designing and implementing these technical safeguards, which may include cryptographic protections techniques.

Parameter Value(s):

#1 "Cryptographic protection of stored cryptographic keys, device certificates, configuration data, and audit logs."

#2 "all systems"

Standard: NTCIP 1218 [Section 3.6.1.2.1]⁹

⁸ <https://www.arc-it.net/html/security/controlsclarification.html>

⁹ <https://www.ntcip.org/file/2025/01/NTCIP-1218-v01A-2024-AsPublished.pdf>

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: The manufacturer ensures that cryptographic keys used to protect information at rest are stored in hardware-backed cryptographic modules that prevent unauthorized extraction or misuse. Keys are generated, stored, and destroyed in accordance with applicable key management policies.

Parameter Value(s):

“Hardware-backed cryptographic modules providing non-exportable key storage and tamper response consistent with FIPS 140-3 or equivalent validated security requirements.”

Standards: FIPS 140-3⁽³⁴⁾, NIST SP 800-57 Part 1⁽²⁹⁾, NIST SP 800-111⁽³¹⁾, and ISO/IEC 11889-1:2015⁽³⁹⁾ & 19790:2025⁽⁴⁰⁾

SC-32, System Partitioning

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.

RSUs contain multiple functional components including V2X processing, management interfaces, radio modules, and cryptographic services. Without partitioning, compromise of one component could impact other security-critical functions.

Guidance: The IOO defines partitioning requirements for RSU components based on mission and risk considerations. The manufacturer designs the RSU to support logical or physical partitioning between security-relevant functions and externally exposed interfaces. Security-critical functions such as cryptographic operations and credential storage are isolated from radio interfaces, management services, and diagnostic functions. Controlled interfaces regulate communication between partitions.

Parameter Value(s):

#1 “V2X processing functions, management interfaces, radio communication modules, and cryptographic services.”

#2 “Logical separation using operating system isolation mechanisms or physical separation where required by policy.”

#3 “Security-critical functions isolated from externally accessible interfaces.”

SC-34, Non-Modifiable Executable Programs

Responsible Party (M/I): M

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

Guidance: The manufacturer ensures that critical executable components of the RSU are protected against unauthorized modification. Operating system kernels, bootloaders, and core V2X applications

are stored in read-only memory or are cryptographically verified prior to execution. Updates require signature verification before installation.

Parameter Value(s):

#1 “Bootloader, operating system kernel, V2X application services, and security services.”

paragraph b. “V2X message processing services, certificate validation services, management interface services, and security services.”

SC-35, External Malicious Code Identification

Responsible Party (M/I): M

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

Guidance: The manufacturer implements mechanisms to prevent execution of unauthorized or malicious code introduced via maintenance interfaces, firmware updates, or external communications. Executable content received from external sources is validated using cryptographic signatures prior to execution. Management interfaces restrict code upload functionality to authenticated and authorized users.

SC-39, Process Isolation

Responsible Party (M/I): M

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

Guidance: The manufacturer implements process isolation within the RSU operating environment. Each executing process operates in a separate address space with enforced access controls. Security-sensitive processes such as key management, certificate validation, and firmware verification are isolated from general application processes. Access to protected resources, including signing keys, is restricted to authorized processes only.

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 “Inadequate security policy for ITS” in table 6, Policy and Procedure Vulnerabilities and Predisposing Conditions.

Guidance: Where required by policy, the manufacturer implements hardware-enforced separation for security-critical services, such as cryptographic key storage and firmware integrity validation, using secure elements or equivalent hardware-based isolation mechanisms.

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: The manufacturer implements security protections for RSU wireless interfaces, including Wi-Fi and cellular connectivity. Wireless links use authenticated and encrypted communication mechanisms appropriate to the interface. Default insecure wireless modes are disabled.

Parameter Value(s):

#1: “IEEE 802.11-based Wi-Fi management interfaces; cellular backhaul links (LTE, LTE-V2X, NR-V2X); and V2X radio interfaces.” #2: “Eavesdropping, signal spoofing, replay attacks, man-in-the-middle attacks, rogue access points, session hijacking, and radio frequency interference or jamming.”

Standards: IEEE 802.11a/b/g/n/ac⁽³³⁾, 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: The manufacturer disables unused physical and logical ports by default. Only organization-approved ports required for RSU operation are enabled. The IOO verifies port configurations during deployment and periodic review.

Parameter Value(s):

#1 “physically” #2 “All unused physical ports including UART, I2C, SPI, USB, and diagnostic interfaces.”

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 vulnerabilities in table 6, Conduct an Attack (i.e., direct/coordinate attack tools or activities).

Guidance: The IOO defines restrictions on the use of RSU peripheral interfaces, removable media, and external device connections. The manufacturer designs the RSU to enforce these restrictions through configuration controls and default-disabled features.

Parameter Value(s):

“Peripheral interfaces, removable media, external device ports, and debugging interfaces.”

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: The manufacturer identifies, documents, and communicates security flaws affecting RSU hardware, firmware, or software. The manufacturer provides patches, firmware updates, or documented mitigations. The IOO evaluates updates, tests where feasible, and deploys remediation in accordance with defined timelines. Where patches are not immediately available, compensating controls are implemented.

Parameter Value(s):

paragraph c. “Critical security updates within 30 days of release or sooner based on risk determination; high-risk updates within 60 days; other updates in accordance with organizational risk management policy.”

Risk References and Resources:

ATT&CK for ICS Mitigations / Techniques:

- M0951 / T0820, T0890, T0866, T0862, T0857, T864.

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.

SI-2(4), Flaw Remediation | Automated Patch Management Tools

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 manufacturer enables centralized update mechanisms that allow the IOO to deploy patches in a controlled manner. Automatic vendor-initiated updates are disabled unless explicitly approved. Update deployment supports staged rollout and status reporting.

Parameter Value(s):

"RSU operating system, application services, and security service components."

SI-3, Malicious Code Protection

Responsible Party (M/I): M/I

Justification to Select: Vulnerability "Malware protection not installed or up to date" in table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: The manufacturer implements mechanisms to prevent execution of unauthorized or malicious code, including cryptographic verification of firmware and application updates. Where traditional malware scanning is not feasible, the RSU enforces application allow-listing and signed-code execution. Malicious code detection mechanisms are configured to avoid disruption of safety-critical operations. Alerts are logged and reported for investigation.

Parameter Value(s):

paragraph c.1 #1 monthly"

paragraph c.1 #2 "Endpoints and network entry/exit points".

paragraph c.2 #1 "Block malicious code; send alert to administrator"

paragraph c.2 #2 "Generate audit record and notify security administrator."

Risk References and Resources:

ATT&CK for ICS Mitigations / Techniques:

- M0938 / T0807, T0871, T0849, T0834, T0853
- M0949 / T0864

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.

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 Privileged Users

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Malware protection implemented without sufficient testing” in table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: Only privileged administrators are authorized to modify malicious code protection configurations or update detection mechanisms. The manufacturer ensures update functions require authenticated privileged access and are auditable.

SI-4, System Monitoring

Responsible Party (M/I): M/I

Justification to Select: Vulnerability “Intrusion detection/prevention software not installed” in table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

RSUs operate in exposed environments and communicate over wireless and wired networks. Without monitoring, unauthorized access attempts, configuration changes, anomalous traffic, or credential misuse may go undetected. Monitoring must detect security-relevant events without degrading safety-critical operations.

Guidance: The manufacturer implements monitoring capabilities within the RSU to generate security-relevant audit events, including authentication events, configuration changes, firmware update attempts, certificate validation failures, and anomalous network conditions.

The RSU provides standardized, queryable telemetry to enable integration with IOO monitoring systems. System health data required by NTCIP 1218 (e.g., CPU load, memory availability, storage status, uptime) is provided as operational telemetry but does not replace security monitoring requirements.

The IOO defines monitoring objectives, alert thresholds, review frequency, and integration with centralized monitoring systems. Monitoring mechanisms are configured to avoid adverse impact on V2X performance or safety functions.

Parameter Value(s):

paragraph a.1. “Authentication attempts and failures; configuration changes; firmware update attempts; certificate validation failures; cryptographic module errors; anomalous network traffic patterns; resource exhaustion conditions.”

paragraph b. “Host-based logging and integrity monitoring; centralized log aggregation; anomaly detection; and network monitoring at managed interfaces.”

paragraph g. #1 “Security audit logs, authentication failures, configuration changes, firmware update attempts, certificate lifecycle events, and network anomaly alerts.”

paragraph g. #2 “Security administrators and system administrators.”

paragraph g. #3 “Automated real-time alerting; daily automated review; weekly analyst review.”

Risk References and Resources:

ATT&CK for ICS Mitigations / Techniques:

- M0931 / T0830, T0885, T0884, T0867, T0869

NIST SP 800-82:⁽³⁾ The organization ensures that use of monitoring tools and techniques do not adversely impact the operational performance of the ITS. Example compensating controls include deploying sufficient network, process, and physical monitoring.

ARC-IT Mechanisms:

- Each device should have adequate endpoint malware detection and reporting system deployed. In most cases a software suite of end point protections will include firewalls, antivirus 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) should 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 should 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 should be updated regularly and tuned to properly report security incidents.
- A defined notification and response policy and procedure should 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.

Standard: NTCIP 1218 [Section 3.5.2.1]⁽⁴⁷⁾

SI-4(2), System Monitoring | Automated Tools and Mechanisms for Real-Time Analysis

Responsible Party (M/I): M

Justification to Select: Vulnerability “Intrusion detection/prevention software not installed” in table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: The manufacturer enables the RSU to generate and forward security-relevant events in near real-time to centralized monitoring systems. The IOO deploys automated tools to analyze aggregated events for suspicious activity. Where local real-time analysis is not feasible due to performance constraints, monitoring is performed upstream.

Risk References and Resources:

NIST SP 800-82:⁽³⁾ In situations where the ITS cannot support the use of automated tools to support near-real-time analysis of events, the organization employs compensating controls (e.g., providing an auditing capability on a separate system, non-automated mechanisms or procedures) in accordance with the general tailoring guidance.

ARC-IT Mechanisms: See SI-04.

SI-4(4), System Monitoring | Inbound and Outbound Communications Traffic

Responsible Party (M/I): M/I

Justification to Select: Vulnerability "Lack of integrity checking for communications" in table 6, Communication and Network Configuration Vulnerabilities and Predisposing Conditions.

Guidance: The IOOs should be responsible for defining the frequency of monitoring of inbound and outbound traffic as well as unusual or unauthorized activities and conditions. The manufacturer/vendor should implement logging and reporting mechanisms at the RSU that support the monitoring required by the IOO.

Parameter Value(s):

paragraph b. #1 "weekly"

paragraph b. #2 "intrusion attempts, malware activity, unauthorized configuration changes, anomalous network traffic, and performance degradation"

Risk References and Resources:

ARC-IT Mechanisms: See SI-4.

SI-4(7), System Monitoring | Automated Response to Suspicious Events

Responsible Party (M/I): M/I

Justification to Select: Vulnerability "Intrusion detection/prevention software not installed" in table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: The IOO should define incident response personnel by name and/or role that will be notified automatically of any suspicious events and should define the least disruptive actions to terminate suspicious events. The manufacturer/vendor should implement on the RSU the required automated event notification capability to the centralized event management system that supports automated personnel notifications.

Parameter Value(s):

paragraph a. "Security administrators, System Administrators"

paragraph b. "Generate automated alert; log event; and optionally restrict session or terminate connection in accordance with organizational policy."

SI-4(15), System Monitoring | Wireless to Wireline Communication

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: The manufacturer enables monitoring and logging at the interface where wireless V2X or cellular communications transition to wired cabinet or backhaul networks. The RSU exposes relevant security events and traffic metadata to support detection of anomalous or unauthorized traffic crossing between domains. The IOO implements monitoring infrastructure to analyze this boundary traffic.

SI-7, Software, Firmware, and Information 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.

RSUs operate in exposed roadside environments and rely on firmware, configuration files, cryptographic libraries, and certificate stores to perform safety-critical V2X functions. Unauthorized modification of these elements can undermine authentication, message integrity, and system availability.

Parameter Value(s):

paragraph a. “The RSU operating system, bootloader, communication module firmware, cryptographic libraries, configuration files, and certificate trust stores.”

paragraph b. “Log the incident; generate alert to security administrator; restrict affected functionality; and, where required by policy, restart or enter a restricted operational state.”

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(22) section 3.1.2 if the device supports a basic input/output system.

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

Guidance: The IOO should define software, firmware, and information that requires integrity checks and the time/lifecycle instances when this check is to be performed. The IOO should also define the transitional states or security-relevant events that require integrity checks and the frequency of these checks. The manufacturer/vendor should implement the functionality of integrity checking on the RSU based on the IOOs requirements.

Parameter Value(s):

#1 “Bootloader, operating system, communication module firmware, cryptographic libraries, configuration files, and certificate trust stores.”

#2 “At system startup; upon restart; prior to firmware installation; and upon detection of security-relevant events.”

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 not under configuration management” in table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: The IOO should define the personnel or roles that should receive a notification when an integrity violation occurs at an RSU. The manufacturer/vendor should implement the functionality on the RSU to support integrity violation and log sharing to the centralized system (e.g., TMC) that supports automated personnel/role notifications.

Parameter Value(s):

“Security administrators and system administrators.”

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(6), Software, Firmware, and Information Integrity | Cryptographic Protection

Responsible Party (M/I): M

Justification to Select: Threat “Compromise mission-critical information” in table 3, Exploit and Compromise.

Guidance: The manufacturer implements cryptographic integrity verification mechanisms, such as digital signatures or cryptographic hash validation using keys stored in hardware-protected modules. Integrity validation mechanisms are protected from unauthorized modification.

SI-7(9), Software, Firmware, and Information Integrity | Verify Boot Process

Responsible Party (M/I): M

Justification to Select: Threat “Compromise mission-critical information” in table 3, Exploit and Compromise.

Parameter Value(s):

“The bootloader, operating system kernel, communication module firmware, and security-critical applications.”

Risk References and Resources:

ARC-IT Mechanisms: See SI-7.

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, Exploit and Compromise.

Guidance: The IOO should define the system component(s) that require boot firmware integrity protection at an RSU. The manufacturer/vendor should implement the functionality on the RSU.

Parameter Value(s):

#1 “Bootloader and root-of-trust firmware components.”

#2 “Cryptographic signature verification; hardware-enforced write protection; authenticated update mechanism.”

Risk References and Resources:

ARC-IT Mechanisms: See SI-07.

Standards: NIST SP 800-193⁽²⁷⁾ & SP 800-147⁽³²⁾

SI-7(12), Software, Firmware, and Information Integrity | Integrity Verification

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.

Parameter Value(s):

“RSU firmware images, configuration files, and cryptographic trust stores.”

SI-10, Information Input Validation

Responsible Party (M/I): M

Justification to Select: Threat “Compromise mission-critical information” in table 3, Exploit and Compromise.

RSUs process externally supplied inputs over wireless V2X links, backhaul management channels, and local maintenance interfaces. Improper validation of these inputs could enable malformed message exploitation, buffer overflow, protocol misuse, or unauthorized configuration changes that affect safety-critical functions.

Guidance: The manufacturer implements strict input validation mechanisms within the RSU to ensure all received data conforms to expected structure, length, type, format, and protocol constraints prior to processing. Validation is applied before parsing, storage, or execution to prevent buffer overflow, injection, malformed packet exploitation, or logic manipulation.

Parameter Value(s):

“V2X message payloads (e.g., SAE J2735 structures); IEEE 1609.2 certificate and signature objects; management interface inputs; firmware and configuration update packages; and network protocol inputs received over wireless or backhaul interfaces.”

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: RSUs execute network-facing services and cryptographic functions. Memory corruption vulnerabilities, including buffer overflows or arbitrary code execution, could compromise

safety-critical processing. Memory protection mechanisms reduce the likelihood that software defects or malicious inputs can compromise system integrity.

Guidance: The manufacturer implements operating system and hardware-supported memory protection mechanisms that prevent processes from accessing memory regions outside their allocated boundaries. Security-critical processes, including cryptographic operations and certificate validation, execute within protected memory regions.

Memory protection mechanisms are configured to prevent execution of unauthorized code and to reduce the predictability of memory layouts to mitigate exploitation attempts. These protections are implemented in a manner consistent with embedded system performance constraints.

Parameter Value(s):

“Hardware-enforced data execution prevention; address space layout randomization (ASLR); and memory segmentation or privilege separation enforced by the processor architecture.”

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.

SI-17, Fail-Safe Procedures

Responsible Party (M/I): M/I

Justification to Select: Threat “Loss of Safety” in table 5, Physical Object Threat Events.

Guidance: The IOO defines the failure conditions that require fail-safe behavior, including loss of communication, processing errors, cryptographic validation failures, or internal system faults.

The manufacturer implements logic within the RSU to transition to a predefined safe operational state when those conditions occur. The selected fail-safe state must preserve safety and prevent dissemination of invalid or misleading V2X information. Fail-safe procedures are documented and tested to ensure predictable behavior under fault conditions.

Parameter Value(s):

#1: “Loss of backhaul connectivity to the TMC; loss of V2X radio functionality; repeated cryptographic validation or certificate verification failures; firmware or configuration integrity violation; resource exhaustion affecting message processing; or abnormal system restart.”#2: “Cease transmission of affected V2X messages; transition to predefined safe operational configuration; log the failure event; generate alert to designated operations or security personnel; and perform controlled restart or recovery procedures where appropriate.”

Risk References and Resources:

NIST SP 800-82:⁽³⁾ The selected failure conditions and corresponding procedures may vary among baselines. The same failure event may trigger different responses, depending on the

impact level. Mechanical and analog systems can be used to provide mechanisms to ensure fail-safe procedures. Fail-safe states should incorporate potential impacts to human safety, physical systems, and the environment. Related controls: CP-6.

This control provides a structure for the organization to identify its policy and procedures for dealing with failures and other incidents. Creating a written record of the decision process for selecting incidents and appropriate response is part of risk management in light of the changing environment of operations.

ARC-IT Mechanisms: See SI-7, SC-7, SC-24.

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).

RSUs rely on commercial hardware, firmware, radio modules, and cryptographic components that may be sourced globally. Compromise in the supply chain could introduce malicious functionality or undermine trust anchors.

Guidance: The IOO develops and maintains a Supply Chain Risk Management (SCRM) Plan that addresses acquisition, integration, maintenance, and disposal of RSU components. The plan identifies critical components, defines supplier trust requirements, and establishes review and approval processes.

The IOO may require the RSU manufacturer to maintain its own SCRM program consistent with NIST SP 800-161 and provide relevant documentation during procurement or review.

Parameter Value(s):

paragraph a. “RSU hardware platforms; communication modules; cryptographic modules or secure elements; firmware; and certificate trust stores.”

paragraph b. “At least annually and upon significant supplier, component, or threat landscape changes.”

Standard: NIST SP 800-161⁽²⁶⁾

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 IOO establishes supply chain controls and contractual requirements to ensure integrity, authenticity, and traceability of RSU components. These controls may include supplier

vetting, component traceability, configuration management controls, secure delivery procedures, and documentation requirements.

The IOO may require manufacturers to document internal supply chain controls and provide attestations or evidence of compliance.

Parameter Value(s):

paragraph a. #1 “RSU hardware assemblies; radio modules; cryptographic modules; firmware images; and secure boot components.”

paragraph a. #2 “Supply chain risk management personnel; procurement officials; program managers; and security officers.”

paragraph c. “Supply chain risk management 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 IOO assesses suppliers of critical RSU components to evaluate security posture, development practices, and supply chain protections. Assessments may include documentation review, questionnaires, audit reports, or third-party certifications.

Parameter Value(s):

“At least annually and upon significant security events, supplier changes, or component changes.”

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: This is an organizational control, but the IOO may want to require the RSU manufacturer/vendor to perform testing and analysis for suppliers pertaining to the more critical RSU components.

Parameter Value(s):

#1 “Independent third-party security assessment; independent third-party component or firmware testing; or review of recognized certification reports (e.g., FIPS 140 validation, Common Criteria, or equivalent).”

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 manufacturer designs RSUs with tamper-evident and tamper-detection mechanisms appropriate to roadside deployment, such as sealed enclosures, protected fasteners, and intrusion detection where feasible.

The IOO establishes inspection and response procedures when tampering is suspected.

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: The IOO inspects RSUs upon receipt, during installation, and when tampering indicators or anomalous behavior are observed. Inspections include verification of hardware integrity, firmware authenticity (e.g., digital signature validation), and presence of tamper-evident mechanisms.

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: The IOO establishes procedures for secure disposal or sanitization of RSU hardware and associated storage media. Disposal processes include removal or zeroization of cryptographic keys, certificates, and configuration data prior to transfer, reuse, or destruction.

Chapter 5. Implementation Considerations

Organizations should consider the following control guidance when implementing RSUs that store, process, or transmit ITS information. These considerations focus on exposed roadside deployment environments, embedded firmware integrity, cryptographic trust, and V2X certificate management.

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

Dual authorization should be considered for security-sensitive actions that could materially affect RSU integrity or trust posture. These include firmware installation, secure boot configuration changes, cryptographic key injection, trust anchor updates, and debug interface activation.

Because RSUs may expose hardware interfaces such as UART, I2C, SPI, JTAG, or USB during manufacturing or maintenance, unauthorized physical access could allow privileged operations. Organizations should require two-person authorization or equivalent technical enforcement for high-impact operations such as:

- Enabling debug modes
- Modifying boot configuration
- Injecting cryptographic material
- Performing firmware recovery

Technical enforcement may include hardware-backed authentication, role separation, and cryptographic approval workflows rather than relying solely on procedural controls.

AC-6(8), Least Privilege | Privilege Levels for Code Execution(1), (8), (10)

RSUs should enforce privilege separation between bootloader, operating system kernel, application layer, cryptographic services and management interfaces. Unnecessary kernel modules, debug shells, and legacy service interfaces should be disabled in production builds. Code execution must occur at the lowest necessary privilege level. Firmware update processes must not grant interactive root-level access unless explicitly authorized and authenticated.

CM-2, Baseline Configuration

RSUs must operate from a hardened baseline configuration that disables booting from removable media, unauthenticated recovery modes, debug interfaces in production environments, and any unused services or ports. The baseline configuration defines the secure boot state, approved certificate trust anchors, management interface restrictions, wireless interface configuration, and logging and monitoring settings. This baseline serves as the authoritative security configuration for the device and must be protected from unauthorized modification. The integrity of the baseline configuration should be periodically verified to ensure that no unauthorized changes have occurred over time.

PE-3, Physical Access Control

Cabinets and enclosures must incorporate locking mechanisms appropriate to the deployment environment, tamper-evident seals, and protected fasteners designed to resist casual or opportunistic access. Where risk warrants, intrusion detection mechanisms should be integrated to alert operators of unauthorized access attempts. Physical protections must be layered with logical safeguards so that physical compromise alone does not automatically result in disclosure of cryptographic keys, modification of firmware, or bypass of authentication controls.

SA-10, Develop Configuration Management

Manufacturers must maintain version-controlled configuration baselines covering firmware, secure boot configuration, cryptographic libraries, and trust stores. Firmware builds must be reproducible and cryptographically signed to ensure authenticity and traceability. Configuration management processes must track all security-relevant changes and preserve clearly defined cryptographic boundaries. Security-impacting changes to boot components, certificate handling, or communication stacks must be formally documented, reviewed, and controlled throughout the system lifecycle.

SI-3, Malicious Code Protection

Because RSUs are embedded safety systems, malicious code protection should rely on cryptographic enforcement mechanisms rather than traditional antivirus solutions. Protection is achieved through signed firmware enforcement, application allow-listing, secure boot validation, and authenticated update channels. Traditional antivirus tools are generally inappropriate for embedded and real-time ITS environments due to performance and determinism constraints. Instead, integrity enforcement must be tightly integrated into the boot process and firmware update workflow to prevent unauthorized or modified code from executing.

SI-7(1), Software, Firmware, and Information Integrity | Integrity Checks (1,2,6,9,10,12)

RSUs must verify the integrity of the bootloader, operating system, communication module firmware, cryptographic libraries, configuration files, and certificate trust stores. Integrity verification should occur at

system startup, prior to firmware installation, and following security-relevant events that could affect system state. Hardware-backed cryptographic verification mechanisms, such as signature validation anchored in a protected root of trust, are strongly recommended to prevent tampering and unauthorized modification.

SI-7(9), Software, Firmware, and Information Integrity | Verify Boot Process

Secure boot must be enabled and enforced in all production deployments. The boot chain must cryptographically verify each stage of execution, including the bootloader, kernel, and security-critical applications, before control is transferred. Legacy or fallback boot paths that bypass verification must be disabled. If boot verification fails, the system must transition to a defined secure state that prevents execution of untrusted code and preserves system integrity.

SI-7(10), Software, Firmware, and Information Integrity | Protection of Boot Firmware

Boot firmware and root-of-trust components must be protected from unauthorized modification. These components should be write-protected except during authenticated and integrity-verified update procedures. All firmware updates must be vendor signed, verified prior to installation, and logged for audit purposes. Where supported, SPI flash protections and hardware-enforced write restrictions should be enabled to safeguard the boot chain and prevent persistent compromise.

SC-17, Public Key Infrastructure Certificates

RSUs participating in V2X operations must securely manage public key certificates in accordance with IEEE 1609.2 and applicable SCMS certificate policies. This includes secure generation or provisioning of device key pairs and protection of private keys within secure elements or hardware security modules. Enrollment Certificates must be properly installed and protected, and application certificates must be securely acquired and stored. RSUs must validate inbound certificates by constructing and verifying certificate chains to trusted SCMS root authorities and must process and enforce Certificate Revocation Lists in accordance with SCMS requirements. Certificate Trust Lists must be securely managed and updated through authenticated and integrity-verified processes. Trust stores must be protected from unauthorized modification, and RSUs should maintain reliable connectivity to SCMS components to support certificate lifecycle operations. Improper certificate management can undermine message authenticity even when firmware integrity is intact.

SC-8 Transmission Confidentiality and Integrity

RSUs must provide integrity protection for V2X messages through IEEE 1609.2 digital signatures. Management and backhaul communications must use mutually authenticated Transport Layer Security sessions. All cryptographic mechanisms must comply with applicable federal standards and use approved algorithms. For broadcast V2X safety messages, integrity protection is typically more critical than confidentiality, as the primary risk involves spoofing or message manipulation rather than data disclosure.

SR-9, Tamper Resistance and Detection

RSUs deployed in exposed environments should incorporate tamper resistance and detection mechanisms commensurate with assessed risk. Detection of enclosure breach or tampering with critical components should generate an alert, log the event, and trigger predefined protective actions. In high-assurance deployments, automatic zeroization of cryptographic keys may be considered; however, such measures must be carefully evaluated to avoid unintended denial-of-service conditions that could affect safety or availability.

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⁽²⁾ that could potentially impact RSU's is provided in table 3 (adversarial) and table 4 (non-adversarial) below. The properties of RSU's may also present unique opportunities to a threat source, specifically addressing how the threat source can manipulate the process of the RSU's to cause damage or achieve other malicious purposes (e.g., exfiltration of data). table 4 provides an overview of potential threat events from NISTSP 800-82⁽³⁾ that are more specific to RSU's. Threat events listed below focus on the RSU's (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 RSU's or its mission/operations, either by compromise of the RSU 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 RSU's can implement a protection measure to mitigate the risk will the threat be considered relevant to the RSU 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 and improve the ability to launch successful attacks.
	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.
	Perform reconnaissance and surveillance of targeted organizations.	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 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.

Threat Events	Tactics, Techniques, and Procedures	Description
	Craft counterfeit certificates.	Adversary counterfeits or compromises a certificate authority, so that malware or connections will appear legitimate.
<i>Deliver/Insert/Install Malicious Capabilities</i>	Deliver modified malware to internal organizational information systems.	Adversary uses common delivery mechanisms (e.g., email) 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., web traffic, instant messaging, 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.
	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, though 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.

Threat Events	Tactics, Techniques, and Procedures	Description
	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.
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 organizational information systems in an attempt to compromise the systems before mitigation measures are available or in place.
	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.
	Compromise critical systems via physical access.	Adversary obtains physical access to organizational information systems and makes modifications.
	Compromise 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 software of organizational critical information systems.	Adversary inserts malware or otherwise corrupts critical internal organizational information systems.
	Compromise organizational information systems to facilitate exfiltration of data/information.	Adversary implants malware into internal organizational information systems, where the malware over time can identify and then exfiltrate valuable information.
	Compromise design, manufacture, and/or distribution of system components (including hardware, software, and firmware).	Adversary compromises the design, manufacture, and/or distribution of critical information system components at selected suppliers.
Conduct an Attack (i.e., direct/	Conduct communications interception attacks.	Adversary takes advantage of communications that are either unencrypted or use weak encryption (e.g.,

Threat Events	Tactics, Techniques, and Procedures	Description
<i>coordinate attack tools or activities</i>		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 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 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 physical attacks on infrastructures supporting organizational facilities.	Adversary conducts a physical attack on one or more infrastructures supporting organizational facilities (e.g., breaks a water main, cuts a power line).
	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 internally based session hijacking.	Adversary places an entity within organizations in order to gain access to organizational information systems or networks for the express purpose of taking control (hijacking) an already established, legitimate session either between organizations and external entities (e.g., users connecting from remote locations) or between two locations within internal networks.
	Conduct externally based network traffic modification (man in the middle) attacks.	Adversary, operating outside organizational systems, intercepts/eavesdrops on sessions

Threat Events	Tactics, Techniques, and Procedures	Description
		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.
	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 systems and components.
	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.
	Obtain sensitive information via exfiltration.	Adversary directs malware on organizational systems to locate and surreptitiously transmit sensitive information or insider manually exfiltrates data.
	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 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.

Threat Events	Tactics, Techniques, and Procedures	Description
	Cause integrity loss by injecting false but believable data into organizational information systems.	Adversary injects false but believable data into organizational information systems, resulting in suboptimal actions or loss of confidence in organizational data/services.
<i>Achieve Results (i.e., cause adverse impacts, obtain information)</i>	Obtain information by externally located interception of wireless network traffic.	Adversary intercepts organizational communications over wireless networks. Examples include targeting public wireless access or hotel networking connections, and drive-by subversion of home or organizational wireless routers.
	Obtain information by externally located interception of wireless network traffic.	Adversary intercepts organizational communications over wireless networks. Examples include targeting public wireless access or hotel networking connections, and drive-by subversion of home or organizational wireless routers.
	Obtain unauthorized access.	Adversary with authorized access to organizational systems, gains access to resources that exceeds authorization.
	Obtain information by opportunistically stealing or scavenging information systems/components.	Adversary steals information systems or components (e.g., laptop computers or data storage media) that are left unattended outside of the physical perimeters of organizations, or scavenges discarded components.
<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.

Table 3 provides a high-level characterization of non-adversarial threat events as adapted from NIST SP 800-30.⁽²⁾ 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.
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.
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 RSU than the general threats listed in tables 2 and 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 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.
Loss of availability.	Adversaries may leverage malware to delete or encrypt critical data on human-machine interfaces, workstations, or databases.

Table 6 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 facility 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.

Table 6. Vulnerabilities and Predisposing Conditions

Vulnerability		Description
<i>Policy and Procedure Vulnerabilities and Predisposing Conditions</i>	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.
	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 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 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.
<i>Architecture and Design Vulnerabilities and Predisposing Conditions</i>	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.
	Hardware, firmware, and software not under asset	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

Vulnerability		Description
	management.	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.
Configuration and Maintenance Vulnerabilities and Predisposing Conditions	Hardware, firmware, and software are not under configuration management.	The organization doesn't know the 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 an ITS, there should be an accurate listing or repository of the current configurations.
	OS and vendor software may not be developed until long after security vulnerabilities are found.	Out-of-date OSs and applications may contain newly discovered vulnerabilities that could be exploited. Security support may not be available for legacy OT, so vulnerability management procedures should include contingency plans for mitigating vulnerabilities where may never be available or replacement plans
	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.
	Inadequate access controls applied.	Access controls are 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:

Vulnerability		Description
		• 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
	Denial of service (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.
	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 • 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, electromagnetic pulse (EMP), static discharge, brownouts, and voltage spikes.	Some hardware used for OT systems is vulnerable to radio frequency, electromagnetic pulses (EMP), 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

Vulnerability		Description
	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 Predisposing Conditions	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
	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, File Transfer Protocol (FTP), Hypertext Transfer Protocol (HTTP), and Network File System (NFS). 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.,

Vulnerability		Description
		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.
	Inappropriate segmentation of the asset management system.	Most architectures are designed for PLCs, RTUs, DCS, 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.
Sensor, Final Element, and Asset Management Vulnerabilities and Predisposing Conditions	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 (e.g., Bluetooth, Wi-Fi, Wireless HART). 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.

Appendix B. NIST SP 800-53 Security Control's Mapping

Table 7. Mapping of RSU Mission Objectives to NIST CSF Subcategories and NIST SP 800-53 Controls

Objective	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 RSUs supporting predefined V2I communication functions within ITS processes.
	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-18: Privacy Program Plan PM-30: Supply Chain Risk Management Strategy SR-03: Supply Chain Controls and Processes SR-05: Acquisition Strategies, Tools, and Methods SR-06: Supplier Assessments and Reviews SR-08: Notification Agreements	
	GV.OC-03: Legal, regulatory, and contractual requirements regarding cybersecurity — including privacy and civil liberties obligations — are understood and managed.	2	MA-01: Policy and Procedures MP-01: Policy and Procedures PE-01: Policy and Procedures PL-01: Policy and Procedures	

Objective	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-28: Risk Framing	
	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 managed at the broader transportation network level, not for individual RSUs.
	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-05: Acquisition Strategies, Tools, and Methods	SR-5 was not chosen because acquisition strategies for supply chain risks are organizational, not specific to RSU deployment in the field. PM-30 was not chosen as it focuses on enterprise-level supply chain risk management, which is not directly applicable to RSU operational configurations.
	GV.RM-01: Risk management objectives are established and	3	PM-09: Risk Management Strategy	

Objective	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
	agreed to by organizational stakeholders.		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 managed centrally in ITS, with RSUs handling minimal PII primarily related to vehicle data, not requiring device-level privacy policies.
	GV.RM-07: Strategic opportunities (i.e., positive risks) are characterized and are included in organizational cybersecurity risk discussions.	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	
	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 relevant to RSU device operations. PM-19 was not chosen because privacy leadership roles are organizational and

Objective	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
				not applicable to RSUs, which operate under broader ITS privacy governance. PM-23 was not chosen because data governance is low priority for RSUs, with V2I data managed by central ITS policies rather than requiring a dedicated governance body. PM-24 was not chosen because data integrity for RSU communications is ensured through technical encryption and validation, not necessitating a formal board at the device level. PM-29 was not chosen because risk management leadership is organizational, with RSU risks incorporated into broader ITS strategies.
	GV.OV-01: Cybersecurity risk management strategy outcomes are reviewed to inform and adjust strategy and direction.	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-05: Acquisition Strategies, Tools, and Methods	
	GV.SC-01: A cybersecurity supply chain risk management program, strategy, objectives, policies, and	3	PM-30: Supply Chain Risk Management Strategy	

Objective	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
	processes are established and agreed to by organizational stakeholders.		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 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	AT-1 was not chosen because security awareness and training policies are established at the enterprise level, with RSUs relying on automated operations and minimal operator interaction, negating the need for device-specific policy enforcement. AU-1 was not chosen because audit and accountability policies are managed organizationally, with RSUs leveraging centralized ITS logging systems rather than requiring device-level procedural frameworks. CA-1 was not chosen because security assessment and authorization policies are governed at the enterprise ITS level, with RSUs integrated into broader network evaluations rather than needing stand-alone policies. CM-1 was not chosen because configuration management policies are defined organizationally, with RSUs

Objective	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
			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	adhering to standardized ITS configurations rather than device-specific policy mandates. CP-1 was not chosen because contingency planning policies are orchestrated at the enterprise level, with RSUs supported by ITS-wide redundancy rather than device-specific contingency procedures. IA-1 was not chosen because identification and authentication policies are set at the organizational level, with RSUs using network-based access controls rather than device-specific procedural requirements. MA-1 was not chosen because maintenance policies are managed enterprise-wide, with RSUs following ITS maintenance schedules rather than requiring device-level policy frameworks. MP-1 was not chosen because media protection policies are handled at the organizational level, with RSUs lacking significant removable media or local data storage needs.

Objective	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
				PE-1 was not chosen because physical and environmental protection policies are defined organizationally, with RSUs designed for rugged outdoor deployment under broader ITS physical security standards. PL-1 was not chosen because security planning policies are established at the enterprise level, with RSUs integrated into overarching ITS planning rather than requiring device-specific procedures. PM-1 was not chosen because information security program policies are managed organizationally, with RSUs operating under enterprise-wide ITS security governance. PM-31 was not chosen as it pertains to enterprise-wide monitoring programs, which are broader than the specific monitoring needs for RSUs. PS-1 was not chosen because personnel security policies are established at the enterprise level, with RSU access managed through ITS-wide role-based controls, not device-level policies. PT-1 was not chosen because PII processing and

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

Objective	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
				transparency policies are managed organizationally, with RSUs handling minimal vehicle data under broader ITS privacy frameworks. SA-1 was not chosen because system and services acquisition policies are managed organizationally, with RSU procurement integrated into ITS-wide acquisition strategies. SC-1 was not chosen because system and communications protection policies are orchestrated at the enterprise level, with RSU V2I communications secured through ITS network controls. SR-1 was not chosen because supply chain risk management policies are established at the enterprise level, with RSU vendor relationships managed under broader ITS procurement frameworks.
	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	
	GV.SC-05: Requirements to address cybersecurity risks in	3	SA-04: Acquisition Process SA-09: External System Services	

Objective	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
	supply chains are established, prioritized, and integrated into contracts and other types of agreements with suppliers and other relevant third parties.		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, prioritized, assessed, responded to, and monitored over the course of the relationship.	3	RA-09: Criticality Analysis SA-04: Acquisition Process SA-09: External System Services 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	PM-28 was not chosen because risk framing is an enterprise-level process, integrated into overall ITS risk management rather than RSU-specific.

Objective	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
			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 provisions for activities that occur after the conclusion of a partnership or service agreement.	3	PM-31: Continuous Monitoring Strategy 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	

Objective	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
	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 managed throughout their lifecycles.	3	CM-09: Configuration Management Plan CM-13: Data Action Mapping 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	CM-09 was not chosen as it pertains to developing a comprehensive configuration management plan at the enterprise level, which is broader than the specific configuration controls needed for RSU operational security. CM-13 was not chosen because mapping data actions is not critical for RSUs, as their data flows are predefined and managed by centralized ITS systems, not requiring device-level mapping. PM-22 was not chosen because RSUs handle limited vehicle-related data without long-term PII storage, making quality management controls unnecessary at the device level. SI-12 was not selected as it focuses on data retention policies and disposal, which are not directly relevant to mitigating physical attacks like

Objective	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
				USB booting or SPI tampering on RSUs SI-18 was not chosen because PII quality operations are irrelevant for RSUs, as V2I data is not processed for PII extraction or quality assurance at the device level. SA-03 was not chosen as it addresses the overall system development process, which is less relevant to the operational security of deployed RSUs.
	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-8 was not chosen because privacy impact assessments are conducted at the enterprise level, with RSUs handling minimal PII that is governed by ITS-wide privacy policies. PM-09 was not selected because it applies to enterprise-wide risk management frameworks, which are too high-level for RSU-specific security needs.
	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 initiatives, not device-specific for RSUs focused on V2I data exchange.

Objective	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
				RA-2 was not chosen because security categorization is performed at the ITS system level, with RSUs assigned risk levels within the broader network context, not as stand-alone devices.
	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 disclosures are established.	3	RA-05: Vulnerability Monitoring	
	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	CA-2 was not chosen because periodic control assessments are conducted at the ITS network level, not requiring specific evaluations for RSUs, which focus on reliable V2I communication. CP-2 was not chosen because detailed contingency plans are less critical for RSUs, which rely on network-level failover and distributed deployment for operational continuity.

Objective	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
			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 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	RA-1 was not chosen because risk assessment policies are developed at the enterprise level, with RSU risks evaluated within the broader ITS risk management framework. SA-17(6) was not chosen because testing structures in development are not necessary for RSU operations, which focus on integration testing within ITS networks.

Objective	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
			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 coordination with suppliers and relevant third parties.	3	Same controls as ID.IM-01	
	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-05: Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and	2	AC-03: Access Enforcement AC-05: Separation of Duties AC-06: Least Privilege AC-17: Remote Access	

Objective	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
	incorporate the principles of least privilege and separation of duties.		AC-18: Wireless Access	
	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-04: Access Control For Transmission PE-06: Monitoring Physical Access	
	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 RSUs operate autonomously with limited human interaction, reducing the need for extensive training and awareness programs beyond basic maintenance protocols.
	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	

Objective	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
	PR.IR-02: The organization's technology assets are protected from environmental threats.	2	PE-09: Power Equipment and Cabling PE-11: Emergency Power PE-14: Environmental Controls	
	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	SC-36 was not chosen because RSUs perform localized processing and minimal storage, with distributed functions handled by the broader ITS infrastructure, not requiring device-specific controls. SI-13 was not chosen because SC-24 <i>Fail in Known State</i> provides sufficient guidance for securing failures to the RSU.
	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 RSUs store minimal data locally, making alternate storage sites unnecessary for their real-time V2I communication functions. CP-7 was not chosen because RSUs perform localized processing, with redundancy provided by other RSUs and ITS infrastructure, negating the need for alternate processing sites. CP-08 was not selected because it focuses on ensuring the availability of telecommunications services

Objective	Subcategory	Affinity	NIST SP 800-53 Mapped Controls	Notes
				for continuity of operations, which is not directly relevant to the RSU hardware and firmware vulnerabilities. PM-3 was not chosen because resource allocation for security and privacy is handled at the program level, not specifically for RSU field devices.
	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 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	3	IR-06: Incident Reporting IR-08: Incident Response Plan	SR-8 was not chosen because notification agreements for supply chain issues are

Objective	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
	with relevant third parties once an incident is declared.		SR-03: Supply Chain Controls and Processes SR-08: Notification Agreements	managed at the enterprise level, not for individual RSUs. IR-06 was not selected because it is handled by the SCMS and focuses on enterprise-level reporting processes, not RSU-specific security.
	RS.MA-02: Incident reports are triaged and validated.	3	IR-04: Incident Handling IR-05: Incident Monitoring IR-06: Incident Reporting	IR-05 was not chosen as it is managed within the SCMS and focuses on broader incident tracking not specific to RSU operations.
	RS.MA-03: Incidents are categorized and prioritized.	3	IR-04: Incident Handling IR-05: Incident Monitoring IR-06: Incident Reporting	
	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 as it is part of the SCMS and addresses external support, which is not directly relevant to RSU security controls.
	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 selected because it is managed within the SCMS and pertains to enterprise-level planning, not specific RSU security measures.
	RS.MI-01: Incidents are contained.	3	IR-04: Incident Handling	

Objective	Subcategory	Affinity	NIST SP 800-53 Mapped Controls	Notes
	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	
	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	
	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:	GV.OC-03: Legal, regulatory, and contractual requirements regarding	3	Subcategory/Security Controls are covered in Mission Objective 1	

Objective	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
Increase the Efficiency of the Transportation Ecosystem	cybersecurity—including privacy and civil liberties obligations—are understood and managed.			
	GV.OC-04: Critical objectives, capabilities, and services that external stakeholders depend on or expect from the organization are understood and communicated.	3	Subcategory/Security Controls are covered in Mission Objective 1	
	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 integration is addressed during ITS system design, not as a control for operational RSUs. PL-08 was not chosen because system security architectures are defined at the overarching ITS architecture level (e.g., ARC-IT), not for individual RSU components, to maintain holistic integration.
	ID.AM-08: Systems, hardware, software, services, and data are managed throughout their lifecycles.	3	Subcategory/Security Controls are covered in Mission Objective 1	

Objective	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
	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 removed commensurate with risk.	3	Subcategory/Security Controls are covered in Mission Objective 1	
	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	SC-04 not selected as RSUs do not typically share resources across multiple systems or users in a way that requires specific protections against unauthorized information access beyond existing access controls.
	PR.IR-03: Mechanisms are implemented to achieve resilience	3	Subcategory/Security Controls are covered in Mission Objective 1	

Objective	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
	requirements in normal and adverse situations.			
	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	
	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	3	Subcategory/Security Controls are covered in Mission Objective 1	

Objective	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
	or expect from the organization are understood and communicated.			
	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 into cybersecurity and enterprise risk management, risk assessment, and improvement processes.	3	Subcategory/Security Controls are covered in Mission Objective 1	
	GV.SC-04: Suppliers are known and prioritized by criticality.	3	Subcategory/Security Controls are covered in Mission Objective 1	

Objective	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
	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, responded to, and monitored over the course of the relationship.	3	Subcategory/Security Controls are covered in Mission Objective 1	
	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	

Objective	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
	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 metadata for designated data types are maintained.	3	CM-12: Information Location CM-13: Data Action Mapping SI-12: Information Management and Retention	CM-12 was not chosen because tracking the location of sensitive information is less relevant for RSUs, which primarily handle transient V2I data with minimal on-device storage.
	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	SA-15(7) was not chosen because automated vulnerability analysis in development is not applicable to operational RSUs, which rely on periodic firmware updates for security. SA-15(8) was not chosen because reusing threat information in development is handled by RSU manufacturers, not required for ITS-deployed RSU maintenance.

Objective	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
			SI-04: System Monitoring 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-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-8 was not chosen because RSUs primarily authenticate vehicular systems via standardized V2I protocols, not requiring complex non-organizational user authentication processes. IA-04 was not selected because RSUs do not heavily rely on managing user or device identifiers beyond existing V2X protocol requirements.

Objective	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
			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-08 was not chosen as RSUs primarily interact with devices (e.g., OBUs) rather than non-organizational users requiring direct authentication. IA-10 was not chosen because adaptive authentication is not applicable to RSU, as basic authentication mechanisms are covered in other security controls.
	PR.AA-02: Identities are proofed and bound to credentials based on the context of interactions.	2	IA-12: Identity Proofing	
	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) IA-09: Service Identification and Authentication IA-10: Adaptive Authentication IA-11: Re-authentication	

Objective	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
	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 was not added to the list of security controls since it was withdrawn from NIST SP 800-53r5. ⁽¹⁾ Did not include AC-19: <i>Access Control For Mobile Devices</i> due to it's not being applicable to the RSU 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	
	PR.DS-01: The confidentiality, integrity, 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	MP-8 was not chosen because media downgrading is irrelevant for RSUs, which do not handle classified or sensitive media requiring sanitization processes.

Objective	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
			SI-03: Malicious Code Protection SI-04: System Monitoring SI-07: Software, Firmware, and Information Integrity	
	PR.DS-02: The confidentiality, integrity, and availability of data-in-transit are protected.	3	AU-16: Cross-Organizational Audit Logging CA-03: Information Exchange 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	SC-16 not chosen because it is satisfied within the SCMS for V2X communications and does not address the physical access vulnerabilities specific to RSUs.
	PR.DS-10: The confidentiality, integrity, and availability 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	

Objective	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.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	

Objective	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	
	PR.IR-01: Networks and environments are protected from unauthorized logical access and usage.	3	Subcategory/Security Controls are covered in Mission Objective 2	
	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 ensure availability is maintained.	2	Subcategory/Security Controls are covered in Mission Objective 1	
	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	

Objective	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
			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	
	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 collected, and their integrity and provenance are preserved.	3	Subcategory/Security Controls are covered in Mission Objective 1	
	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	3	CP-02: Contingency Plan CP-04: Contingency Plan Testing	

Objective	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
	assets is verified before using them for restoration.		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 operating status is confirmed.	3	Subcategory/Security Controls are covered in Mission Objective 2	
Mission Objective #7: Enhance the Integration and Connectivity of the Transportation System through Technology	GV.OC-01: The organizational mission is understood and informs cybersecurity risk management.	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	
	GV.OC-05: Outcomes, capabilities, and services that the organization depends on are understood and communicated.	3	Subcategory/Security Controls are covered in Mission Objective 1	
	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	

Objective	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
	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-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-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-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	3	Subcategory/Security Controls are covered in Mission Objective 2	

Objective	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
	communication and internal and external network data flows are maintained.			
	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-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	
	ID.AM-08: Systems, hardware, software, services, and data are managed throughout their lifecycles.	3	Subcategory/Security Controls are covered in Mission Objective 1	
	ID.RA-01: Vulnerabilities in assets are identified, validated, and recorded.	3	Subcategory/Security Controls are covered in Mission Objective 3	
	ID.RA-03: Internal and external threats to the organization are identified and recorded.	3	PM-12: Insider Threat Program PM-16: Threat Awareness Program RA-03: Risk Assessment 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	3	Subcategory/Security Controls are covered in Mission Objective 1	

Objective	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
	to understand inherent risk and inform risk response prioritization.			
	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-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.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-02: Identities are proofed and bound to credentials based on the context of interactions.	2	IA-12: Identity Proofing	
	PR.AA-03: Users, services, and hardware are authenticated.	3	Subcategory/Security Controls are covered in Mission Objective 3	
	PR.AA-04: Identity assertions are protected, conveyed, and verified.	3	IA-13: Identity Providers and Authorization Servers	
	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	3	Subcategory/Security Controls are covered in Mission Objective 1	

Objective	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
	that they possess the knowledge and skills to perform general tasks with cybersecurity risks in mind.			
	PR.DS-01: The confidentiality, integrity, and availability of data at rest are protected.	2	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	An affinity score of 2 is assumed for Mission Objective 7, instead of 1, to reflect the level of v1.1's PR.PT-2.
	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	

Objective	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
			CM-09: Configuration Management Plan CM-10: Software Usage Restrictions CM-11: User-Installed Software	
	PR.PS-03: Hardware is maintained, replaced, and removed commensurate with risk.	3	Subcategory/Security Controls are covered in Mission Objective 1	
	PR.PS-06: Secure software development practices are integrated, and their performance is monitored throughout the software development lifecycle.	3	SA-03: System Development Lifecycle SA-08: Security and Privacy Engineering Principles SA-10: Developer Configuration Management SA-11: Developer Testing and Evaluation SA-15: Development Process, Standards, and Tools SA-17: Developer Security and Privacy Architecture and Design	SA-15 was not chosen because development process standards are applied during RSU vendor selection, not as ongoing controls for deployed systems in the field.
	PR.IR-01: Networks and environments are protected from unauthorized logical access and usage.	3	Subcategory/Security Controls are covered in Mission Objective 2	
	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	

Objective	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
	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.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	
	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	
Mission Objective #8: Build Privacy	GV.OC-02: Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk	3	Subcategory/Security Controls are covered in Mission Objective 1	

Objective	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
Protections into ITS Operations	management are understood and considered.			
	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, communicated, understood, and enforced.	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-24: Data Integrity Board PM-29: Risk Management Program Leadership Roles	PM-13 was not chosen because workforce management for security and privacy is low priority due to RSUs' automated operations with minimal personnel involvement.
	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	

Objective	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
			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	
	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	

Objective	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
	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	
	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	
	PR.AA-04: Identity assertions are protected, conveyed, and verified.	3		

Objective	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
	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: The confidentiality, integrity, and availability of data at rest are protected.	3	Subcategory/Security Controls are covered in Mission Objective 3	
	PR.DS-02: The confidentiality, integrity, and availability of data-in-transit are protected.	3	Subcategory/Security Controls are covered in Mission Objective 3	
	PR.DS-10: The confidentiality, integrity, and availability 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 SA-08: Security and Privacy Engineering Principles SC-04: Information In Shared System Resources SC-07: Boundary Protection	

Objective	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
			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 unauthorized logical access and usage.	3	Subcategory/Security Controls are covered in Mission Objective 3	
	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	

Objective	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
	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	
	RS.MI-02: Incidents are eradicated.	3	Subcategory/Security Controls are covered in Mission Objective 1	
Mission Objective 10: Maintain Secure Technology (Information Technology/OT) and Communications	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	
	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 1	
	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	

Objective	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
	GV.RR-01: Organizational leadership is responsible and accountable for cybersecurity risk and fosters a culture that is risk-aware, ethical, and continually improving.	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 Role	
	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.PO-01: Policy for managing cybersecurity risks is established based on organizational context, cybersecurity strategy, and priorities and is communicated and enforced.	3	Subcategory/Security Controls are covered in Mission Objective 8	
	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	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	3	PM-09: Risk Management Strategy PM-19: Privacy Program Leadership Role	

Objective	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
	of organizational requirements and risks.		PM-30: Supply Chain Risk Management Strategy PM-31: Continuous Monitoring Strategy RA-07: Risk Response SR-06: Supplier Assessments and Reviews	
	GV.OV-03: Organizational cybersecurity risk management performance is evaluated and reviewed for adjustments needed.	3	PM-04: Plan of Action and Milestones Process PM-06: Measures of Performance RA-07: Risk Response SR-06: Supplier Assessments and Reviews	
	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 2	

Objective	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
	ID.AM-05: Assets are prioritized based on classification, criticality, resources, and impact on the mission.	3	Subcategory/Security Controls are covered in Mission Objective 7	
	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	
	ID.RA-07: Changes and exceptions are managed, assessed for risk impact, recorded, and tracked.	3	Subcategory/Security Controls are covered in Mission Objective 7	
	ID.IM-01: Improvements are identified from evaluations.	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 7	
	PR.AA-03: Users, services, and hardware are authenticated.	3	Subcategory/Security Controls are covered in Mission Objective 3	
	PR.AA-04: Identity assertions are protected, conveyed, and verified.	3	Subcategory/Security Controls are covered in Mission Objective 8	
	PR.AA-05: Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and	3	Subcategory/Security Controls are covered in Mission Objective 3	

Objective	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
	incorporate the principles of least privilege and separation of duties			
	PR.AA-06: Physical access to assets is managed, monitored, and enforced commensurate with risk.	3	PE-02: Physical Access Authorizations PE-03: Physical Access Control PE-04: Access Control For Transmission PE-05: Access Control For Output Devices PE-06: Monitoring Physical Access PE-08: Visitor Access Records PE-18: Location of System Components PE-19: Information Leakage PE-20: Asset Monitoring and Tracking	PE-5 was not chosen because RSUs lack direct output devices like displays, with data transmitted to vehicles or central systems, making output device access control unnecessary. PE-8 was not chosen because RSUs are unmanned field devices, and visitor access records are managed at ITS facilities rather than at roadside locations. PE-19 was not chosen because RSUs use encrypted V2I communications, and information leakage risks are mitigated through network-level controls rather than device-specific measures. PE-20 was not selected because it is covered by PE-18 and is less relevant to the specific security requirements of RSUs.
	PR.AT-01: Personnel are provided with awareness and training so that they possess the knowledge and skills to.	3	Subcategory/Security Controls are covered in Mission Objective 1	

Objective	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
	PR.DS-01: The confidentiality, integrity, and availability of data at rest are protected.	3	Subcategory/Security Controls are covered in Mission Objective 3	
	PR.DS-02: The confidentiality, integrity, and availability 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	Subcategory/Security Controls are covered in Mission Objective 7	
	PR.PS-02: Software 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	
	PR.PS-03: Hardware is maintained, replaced, and removed commensurate with risk.	3	Subcategory/Security Controls are covered in Mission Objective 1	
	PR.PS-04: Log records are generated and made available for continuous monitoring.	3	Subcategory/Security Controls are covered in Mission Objective 3	
	PR.PS-05: Installation and execution of unauthorized software are prevented.	3	Subcategory/Security Controls are covered in Mission Objective 1	
	PR.IR-01: Networks and environments are protected from	3	Subcategory/Security Controls are covered in Mission Objective 3	

Objective	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	
	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 collected, and their integrity and provenance are preserved.	3	Subcategory/Security Controls are covered in Mission Objective 3	
	RS.CO-02: Internal and external stakeholders are notified of incidents.	3	Subcategory/Security Controls are covered in Mission Objective 1	
	RS.MI-01: Incidents are contained.	3	Subcategory/Security Controls are covered in Mission Objective 1	
	RS.MI-01: Incidents are contained.	3	Subcategory/Security Controls are covered in Mission Objective 1	
	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	

Objective	Subcategory	Affinity	NIST SP 800-53 Mapped Controls	Notes
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 8	
	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 10	
	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 organizational requirements and risks.	3	Subcategory/Security Controls are covered in Mission Objective 10	
	GV.OV-03: Organizational cybersecurity risk management performance is evaluated and reviewed for adjustments needed.	3	Subcategory/Security Controls are covered in Mission Objective 10	
	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	
	GV.OV-01: Cybersecurity risk management strategy outcomes	3	Subcategory/Security Controls are covered in Mission Objective 1	

Objective	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
	are reviewed to inform and adjust strategy and direction.			
	GV.OV-02: The cybersecurity risk management strategy is reviewed and adjusted to ensure coverage of organizational requirements and risks.	3	Subcategory/Security Controls are covered in Mission Objective 10	
	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 2	
	ID.AM-04: Inventories of services provided by suppliers are maintained.	3	Subcategory/Security Controls are covered in Mission Objective 7	
	ID.AM-05: Assets are prioritized based on classification, criticality, resources, and impact on the mission.	3	Subcategory/Security Controls are covered in Mission Objective 7	
	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	

Objective	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
	ID.RA-07: Changes and exceptions are managed, assessed for risk impact, recorded, and tracked.	3	Subcategory/Security Controls are covered in Mission Objective 7	
	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	
	PR.AA-04: Identity assertions are protected, conveyed, and verified	3	Subcategory/Security Controls are covered in Mission Objective 8	
	PR.DS-01: The confidentiality, integrity, and availability of data at rest are protected.	3	Subcategory/Security Controls are covered in Mission Objective 3	
	PR.DS-02: The confidentiality, integrity, and availability 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	Subcategory/Security Controls are covered in Mission Objective 7	
	PR.PS-04: Log records are generated and made available for continuous monitoring.	3	Subcategory/Security Controls are covered in Mission Objective 1	
	PR.IR-01: Networks and environments are protected from unauthorized logical access and usage.	3	Subcategory/Security Controls are covered in Mission Objective 2	

Objective	Subcategory	Affinity	NIST SP 800-53 Mapped Controls	Notes
	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-09: Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events.	3	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	
	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.AN-07: Incident data and metadata are collected, and their integrity and provenance are preserved.	3	Subcategory/Security Controls are covered in Mission Objective 1	
	RC.RP-01: The recovery portion of the incident response plan is	3	Subcategory/Security Controls are covered in Mission Objective 1	

Objective	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
	executed once initiated from the incident response process.			
	RC.RP-02: Recovery actions are selected, scoped, prioritized, and performed.	3	Subcategory/Security Controls are covered in Mission Objective 1	

Appendix C. Acronyms

ARC-IT	Architecture Reference for Cooperative and Intelligent Transportation
C-I-A	confidentiality, integrity, availability
CSF	Cybersecurity Framework
CTI	Connected Transportation Interoperability
CVRSE	connected vehicle roadside equipment
DoS	denial of service
FIPS	Federal Information Processing Standards
HTTPS	Hypertext Transfer Protocol Secure
ICS	industrial control system
ID	identification
IDS	intrusion detection system
IEEE	Institute of Electrical and Electronics Engineers
IOO	infrastructure owner-operator
IPS	intrusion protection system
ITE	Institute of Transportation Engineers
ITS	Intelligent Transportation Systems
L-M-H	low, moderate, high
NEMA	National Electrical Manufacturers Association
NIST	National Institute of Standards and Technology
NTCIP	National Transportation Communications for ITS Protocol
OT	operational technology
PKI	public key infrastructure
PV	parameter value
RSCE	roadside cabinet electronics
RSU	roadside unit
SCMS	security credential management system
SP	Special Publication

TMC	traffic management center
TMS	traffic management system
TSC	traffic signal controller
V2X	vehicle-to-everything
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
PL	Planning
PM	Program Management
PS	Personnel Security
PT	PII Processing and Transparency
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

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.
cost/benefit analysis	The process of comparing the projected or estimated costs and benefits (or opportunities) associated with a project decision to determine whether it makes sense from a business perspective. For security and privacy, it is necessary to balance the cost of applying selected controls and benefits gained by reducing risk to an acceptable level.
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.
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 traffic management center manager is a component of State department of transportation 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).
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. ITS 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.

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. 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.
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. U.S. Department of Transportation. n.d. "Architecture Reference for Cooperative and Intelligent Transportation." ARC-IT Version 9.3. The National ITS Reference Architecture. <https://www.arc-it.net/index.html>, last accessed October 10, 2025.
6. American Association of State Highway and Transportation Officials (AASHTO), Institute of Transportation Engineers (ITE), National Electrical Manufacturers Association (NEMA), and SAE International. 2022. *Roadside Unit (RSU) Standard Amendment*. Connected Transportation Interoperability (CTI) 4001 v01.01. Published September 2022. <https://www.ite.org/ITEORG/assets/File/Standards/CTI%204001v0101-amended.pdf>, last accessed October 10, 2025.
7. ARC-IT Version 9.3. n.d. "Device Classes." The National ITS Reference Architecture. <https://www.arc-it.net/html/security/deviceclasses.html>, last accessed October 10, 2025.
8. The MITRE Corporation. 2025. "ICS Matrix." MITRE ATT&CK for Industrial Control Systems. Bedford, Massachusetts, and McLean, Virginia. <https://attack.mitre.org/matrices/ics/>, last accessed October 10, 2025.
9. 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.
10. American Association of State Highway and Transportation Officials (AASHTO), Institute of Transportation Engineers (ITE), National Electrical Manufacturers Association (NEMA), and SAE International. 2022. *Roadside Unit (RSU) Standard*. Connected Transportation Interoperability (CTI) 4001 v01.00. Published September 2022.
11. ARC-IT Version 9.3. n.d. "Service Packages." The National ITS Reference Architecture. <https://www.arc-it.net/html/servicepackages/servicepackages-areasort.html>, last accessed October 10, 2025.

12. ARC-IT Version 9.3. n.d. "Security." The National ITS Reference Architecture. <https://www.arc-it.net/html/security/security.html>, last accessed October 10, 2025.
13. National Institute of Standards and Technology. 2011. *Managing Information Security Risk: Organization, Mission, and Information System View*. NIST SP 800-39. Washington, DC. U.S. Department of Commerce. <https://csrc.nist.gov/pubs/sp/800/39/final>, last accessed October 15, 2025.
14. 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.
15. 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.
16. Institute of Electrical and Electronics Engineers (IEEE). 2016. *IEEE Standard for Wireless Access in Vehicular Environments – Security Services for Applications and Management Messages*. IEEE Standard 1609.2-2016 (superseded). Published March 1, 2016. https://standards.ieee.org/standard/1609_2-2016.html, last accessed October 10, 2025.
17. SAE International. 2009. *Dedicated Short-Range Communications (DSRC) Message Set Dictionary J2735™_202309*. Warrendale, Pennsylvania: SAE International, issued September 22, 2023.
18. SAE International. 2020. *Ob-Board System Requirements for V2V Safety Communications J2945™*. Warrendale, Pennsylvania: SAE International, issued April 29, 2020.
19. Institute of Electrical and Electronics Engineers (IEEE). 2020. *IEEE Standard for Wireless Access in Vehicular Environments (WAVE)--Certificate Management Interfaces for End Entities*. IEEE Standard 1609.2.1-2020 (superseded). <https://ieeexplore.ieee.org/document/9311462>, last accessed October 15, 2025.
20. Internet Engineering Task Force (IETF). 2018. *The Transport Layer Security (TLS) Protocol Version 1.3*. Request for Comment 8446. RCF Editor. August 2018. <https://www.rfc-editor.org/rfc/rfc8446>, last accessed October 15, 2025.
21. Internet Engineering Task Force (IETF). 2008. *The Transport Layer Security (TLS) Protocol Version 1.2*. Request for Comment 5246. RCF Editor. August 2008. <https://www.ietf.org/rfc/rfc5246.txt>, last accessed October 15, 2025.
22. 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.
23. 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 November 4, 2025.

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

24. 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.
25. 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.
26. 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.
27. 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.
28. 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/800/193/final>, last accessed November 4, 2025.
29. 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.
30. 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.
31. 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.
32. 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.
33. Institute of Electrical and Electronics Engineers (IEEE). 2021. *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 Standard 802.11-2020, published February 2021. <https://ieeexplore.ieee.org/document/9363693>, last accessed November 4, 2025.
34. 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 November 4, 2025.

35. National Institute of Standards and Technology. 2023. *Security Requirements for Cryptographic Modules. Federal Information Processing Standard Publication FIPS PUB 197*. Issued May 09, 2023. Washington, DC. U.S. Department of Commerce. <https://csrc.nist.gov/pubs/fips/197/final>, last accessed November 4, 2025.
36. National Institute of Standards and Technology. 2025. *Digital Identity Guidelines: Authentication and Authenticator Management*. NIST SP 800-63B. Published July 2025. Washington, DC. U.S. Department of Commerce. <https://csrc.nist.gov/pubs/sp/800/63/b/4/final>, last accessed November 4, 2025.
37. Connected Transportation Interoperability (CTI) Technical Committee. 2022. *CTI 4001 v1.0 – Amendment 1. Roadside Unit Standard A connected intersection-ready Standard of AASHTO, ITE, NEMA and SAE International*, published September 2022. <https://www.ite.org/ITEORG/assets/File/Standards/CTI%204001v0101-amended.pdf>, last accessed November 4, 2025.
38. Network Working Group. 2008. *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. RCF Editor. May 2008. <https://www.rfc-editor.org/rfc/rfc5280>, last accessed November 4, 2025.
39. 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.
40. 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.
41. 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.
42. 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.
43. Institute of Electrical and Electronics Engineers (IEEE). 2014. *IEEE Standard for Ethernet*. IEEE Standard 802.3-2018, published June 2014. <https://standards.ieee.org/ieee/802.1X/7345/>, last accessed November 4, 2025.)
44. International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC). 2022. *Information security, cybersecurity and privacy protection — Information security controls*. ISO/IEC 27001:2022, published February 2022. <https://www.iso.org/standard/82423.html>, last accessed November 4, 2025.
45. National Institute of Standards and Technology. 2023. *Standards for Security Categorization of Federal Information and Information Systems FIPS PUB 199*. Issued March 17, 2023. Washington, DC. U.S. Department of Commerce. <https://csrc.nist.gov/pubs/fips/199/final>, last accessed November 4, 2025.

46. 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.
47. National Transportation Communications for ITS Protocol (NTCIP). 2020. *National Transportation Communications for ITS Protocol Object Definitions for Roadside Units (RSUs)*. NTCIP 1218 v01.38. American Association of State Highway and Transportation Officials (AASHTO). December 2020. <https://www.ntcip.org/file/2021/01/NTCIP-1218v0138-RSU-toUSDOT-20200905.pdf>, last accessed February 2026.
48. 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.
49. SAE International. 2018. *V2I System Requirements J2945/2™*. Warrendale, Pennsylvania: SAE International, issued October 30, 2018.
50. SAE International. 2022. *LTE-V2X C-V2X System Profile, J3161/1™*. Warrendale, Pennsylvania: SAE International, issued March 20, 2022.
51. Institute of Electrical and Electronics Engineers (IEEE). 2023. *IEEE Standard for Wireless Access in Vehicular Environments (WAVE) -- Networking Services*. IEEE 1609.3-2023, published January 2016. <https://ieeexplore.ieee.org/document/STDBN20162>, last accessed November 4, 2025.
52. Institute of Electrical and Electronics Engineers (IEEE). 2019. *IEEE Standard for Wireless Access in Vehicular Environments (WAVE)--Identifiers*. IEEE 1609.12-2019, published October 2019. <https://ieeexplore.ieee.org/document/8877516>, last accessed November 4, 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-26-003



U.S. Department of Transportation