

Intelligent Transportation Systems (ITS) Security Control Set for Closed- Circuit Television

www.its.dot.gov/index.htm

Final Report – April 2026
FHWA-JPO-26-002



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-26-002		2. Government Accession No.		3. Recipient's Catalog No.	
4. Title and Subtitle Intelligent Transportation Systems (ITS) Security Control Set for Closed-Circuit Television				5. Report Date April 2026	
				6. Performing Organization Code	
7. Author(s) Brian Russell, Elijah Pichler, Reilly Fastring, Robert Sanchez (ORCID: 0000-0002-0763-6146)				8. Performing Organization Report No.	
9. Performing Organization Name and Address Leidos Inc. 1750 Presidents Street Reston, VA 20190				10. Work Unit No. (TRAIS)	
				11. Contract or Grant No. 693JJ322A000005	
12. Sponsoring Agency Name and Address Federal Highway Administration 1200 New Jersey Avenue, SE Washington, DC 20590				13. Type of Report and Period Covered Final Report, October 2024 – July 2026	
				14. Sponsoring Agency Code ITS JPO	
15. Supplementary Notes The Task Order Contracting Officer Representative for this project was Joe Gregory.					
16. Abstract This control set document identifies cybersecurity controls designed to mitigate risk to closed-circuit televisions (CCTV) operating in the role of ITS roadway equipment described by the Traffic Information Dissemination service package in the Architecture Reference for Cooperative and Intelligent Transportation (ARC-IT) TM06. The objective of this control set is to provide a means to better protect CCTV's and their information flows. Cybersecurity 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 245	
				22. Price N/A	

Table of Contents

Chapter 1. Identification.....	1
Chapter 2. Physical Object Characteristics.....	5
Chapter 3. Summary of Control Specifications	13
Chapter 4. Detailed Control Specifications	33
Chapter 5. Implementation Considerations	169
Appendix A. Threats, Vulnerabilities, and Predisposing Conditions.....	173
Appendix B. NIST SP 800-53 Security Control’s Mapping.....	189
Appendix C. Abbreviations.....	229
Appendix D. Control Family Abbreviations	231
Appendix E. Glossary	233
References.....	235

List of Tables

Table 1. Physical Object Device Security Class by Service Package	8
Table 2. Control Specifications by Device Security Class CCTV	14
Table 3. Adversarial Threat Events	173
Table 4. Non-Adversarial Threat Events	178
Table 5. Physical Object Threat Events	180
Table 6. Vulnerabilities and Predisposing Conditions	181
Table 7. Mapping of CCTV Mission Objectives to NIST CSF Subcategories and NIST SP 800-53 Controls	189

List of Figures

Figure 1. Diagram. IP-Based CCTV System.....	6
Figure 2. Diagram. Analog-Based CCTV System	6

Chapter 1. Identification

Purpose, Scope, and Applicability

This control set document defines the security and privacy controls necessary to address risks specific to closed-circuit television (CCTV) systems within intelligent transportation systems (ITS). Aligned with the TM-01 Traffic Surveillance service package in the Architecture Reference for Cooperative and Intelligent Transportation (ARC-IT)⁽¹⁾, this control set helps ensure the protection of CCTV assets and their associated information flows - including traffic images, traffic image metadata, video surveillance control, and video surveillance coordination.

Derived from National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53,⁽²⁾ these controls focus on safeguarding the confidentiality, integrity, and availability of CCTV assets and their associated information flows. As CCTV technology evolves to include advanced features, this control set aims to mitigate risks inherent to CCTV operations and interfaces, helping to ensure robust, secure video capture, storage, and transmission.

Designed for use by system owners, managers, integrators, engineers, and manufacturers, this control set offers a structured approach to identifying security requirements for CCTV systems. The outlined controls are primarily technical in nature – complement broader ITS security measures and include necessary organizational controls from NIST SP 800-53⁽²⁾ relevant to the design, implementation, and operational support of CCTV systems. Additionally, these controls help address residual risks from overarching ITS infrastructures that may impact CCTV systems, thereby protecting unauthorized access, video manipulation, and service disruptions. By referencing the broader security posture of ITS systems, CCTV stakeholders can identify gaps and apply controls specific to CCTV systems to mitigate unaddressed risks.

This proactive approach helps ensure that critical non-technical controls essential to CCTV security are integrated – whether by manufacturers, infrastructure operators, or organizational stakeholders, to maintain secure, resilient ITS environments. The controls relevant to CCTV systems 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 infrastructure owner/operators (IOOs), system integrators, system engineers, and system component manufacturers to derive security requirements for CCTV systems.

The risk of mitigation and protection provided by other controls implemented in larger systems, operations, or data centers, or by the IOOs operating ITS, benefit physical objects that are part of these larger systems. Owners, operators, and users of CCTV systems may examine the security assessment of the larger system to determine which risks might not be mitigated or might be passed on to CCTV systems themselves and then select controls that mitigate those risks. Some controls tagged in NIST SP 800-53⁽²⁾ as organizational controls are included in this control set because aspects of those controls must 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 CCTV system. Such controls are addressed by the IOO before, during, or after a CCTV system is delivered and installed.

The scope of this control set focuses on how a typical CCTV system would be implemented by the ITS community for common use cases using today's technology. The effort is to identify and select controls applicable to most CCTV implementations. Nuances of other implementations (e.g., legacy, 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 800-53, *Security and Privacy Controls for Information Systems and Organizations*.⁽²⁾
- NIST issues new revisions of NIST SP 800-30, *Guide for Conducting Risk Assessments*.⁽³⁾
- NIST issues new revisions of NIST SP 800-82, *Guide to Industrial Control Systems (ICS) Security*.⁽⁴⁾
- NIST issues new revisions of the Cybersecurity Framework (CSF).⁽⁵⁾
- ARC-IT is significantly revised.
- Relevant standards are developed or updated.
- Significant changes to technologies have been made.
- New threats and/or vulnerabilities are discovered that affect the subject of this document.

Sources

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

- ARC-IT version 9.3,⁽⁶⁾ 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.
- NIST SP 800-30 Revision 1,⁽³⁾ for typical threat sources and vulnerabilities that may be relevant or tailored to apply to ITS.
- NIST SP 800-82 Revision 3,⁽⁴⁾ for ICS threats and vulnerabilities that may be relevant or tailored to apply to ITS.
- MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) version 17.1⁽⁷⁾ for ICS, for threat sources tactics, techniques, and procedures and mitigations that may also be relevant or tailored to ITS.
- MITRE ATT&CK® version 17.1, for enterprise for threat sources' tactics techniques, procedures, and mitigations that may also be relevant or tailored to ITS.

- ITS Cybersecurity Framework Profile 2.0 (ITS Profile)⁽⁵⁾ for prioritizing subcategories mapped to security controls, which can be used to guide control specifications in this control set.

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

The ITS Profile was used to inform the control selections in this document. The ITS Profile identifies and prioritizes ITS mission objectives, which a given system with its physical devices may support. The ITS Profile also aligns functions, categories, and subcategories in the cybersecurity framework core with those mission objectives. Controls that support higher-priority subcategories must be considered for inclusion at each of the five device security class levels⁽⁸⁾ in ARC-IT. 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 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.⁽⁹⁾

Cybersecurity in ARC-IT⁽¹⁰⁾ is addressed through the analysis of the confidentiality, integrity, and availability 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 confidentiality, integrity, and availability dimensions, ARC-IT groups the ratings into five device security classes.⁽⁸⁾ Planners and engineers should select devices that are certified to meet the requirements for a class but 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 CCTV are specified in this control set document. This approach is necessary to simplify and decrease the size of the document and to make it 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 CCTV 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.^(11,12)

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

Chapter 2. Physical Object Characteristics

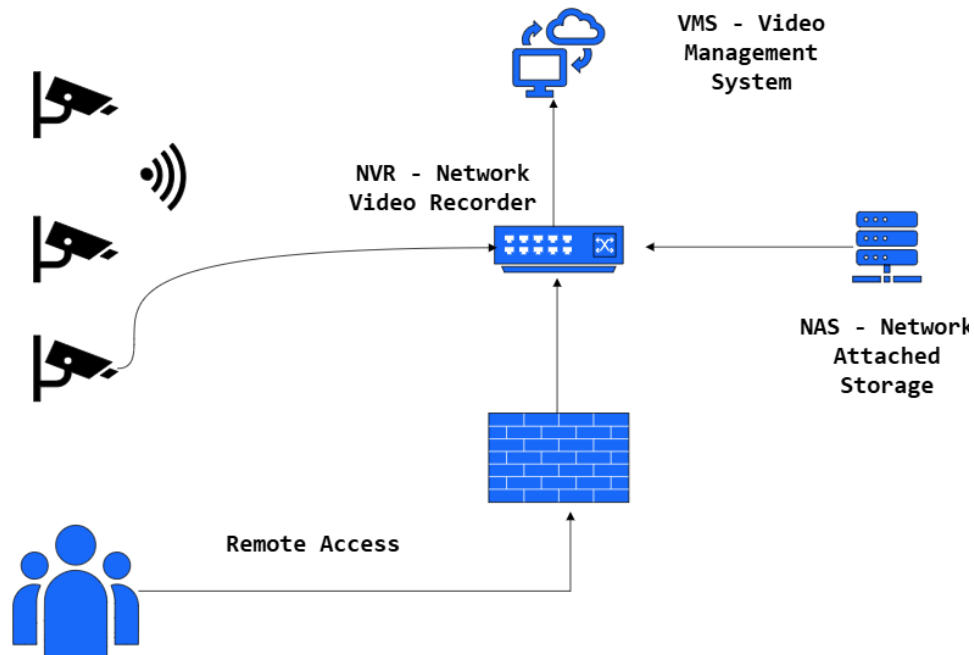
Definition/Description

Closed-circuit television (CCTV) is a system of cameras and associated components used to generate, transmit, display, and store video data for monitoring and surveillance purposes. Within ARC-IT, CCTV operates in the field environment as part of intelligent transportation system (ITS) roadway equipment for video processing. The scope of this control set focuses on ensuring the confidentiality, integrity, and availability of CCTV operations in security, traffic management, and ITS environments by protecting data transmission, maintaining reliable functionality, and preventing unauthorized access or tampering.

CCTV systems operate in both indoor and outdoor environments. Outdoor deployments require durable designs capable of withstanding weather, physical stress, and electromagnetic interference to maintain consistent performance. Architectures vary widely and may include components such as switches, multiplexers, digital video recorders (DVRs), and direct-attached storage (DAS) to support video transmission, storage, and viewing.

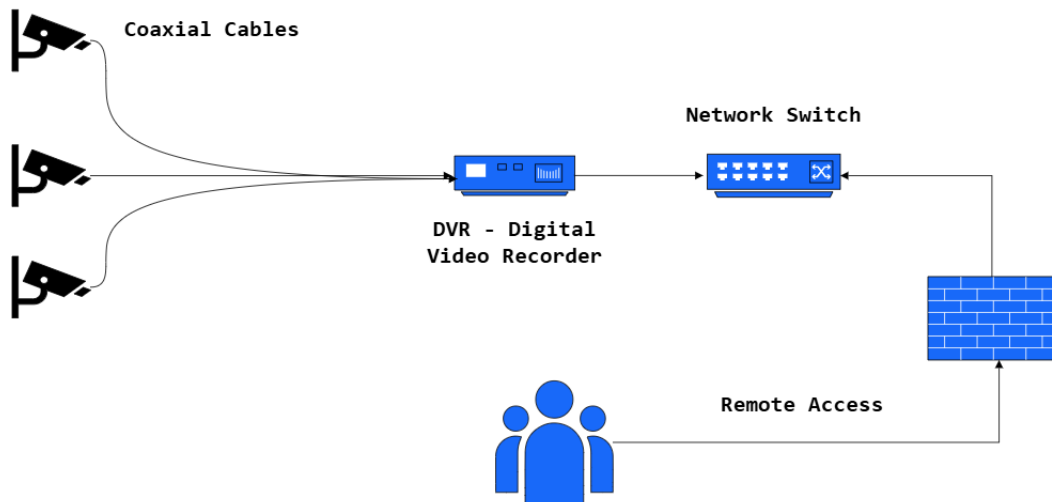
CCTV systems may use either internet protocol (IP) or analog cameras, each with distinct capabilities and cybersecurity considerations. IP-based systems typically operate over local, wide-area, or wireless networks and may use power over Ethernet to deliver both power and data over a single cable. Some architectures rely on dedicated private cabling. Analog systems transmit video over coaxial cables and require DVRs for digitization, generally providing more limited resolution and functionality. IP systems commonly use network video recorders (NVRs) to perform multiplexing and manage video storage. Figures 1 and 2 illustrate representative architectures for both system types.

Figure 1 and figure 2 illustrate the two types of CCTV systems included within the scope of this control set.



Source: TrustThink, 2024

Figure 1. Diagram. IP-Based CCTV System



Source: TrustThink, 2024

Figure 2. Diagram. Analog-Based CCTV System

CCTV system design must incorporate specialized video processing and storage solutions that align with their architectural needs while ensuring effective data retention and accessibility. IP-based CCTV systems often rely on scalable network storage options like network attached storage (NAS), storage area networks (SAN), and DAS, each with distinct security and performance implications.

NAS provides cost-effective file-level access with features like redundant array of independent disks for data protection, while SAN offers high-performance block-level storage using protocols such as Internet Small Computer Systems Interface, ideal for large-scale deployments. Organizations must consider the purpose of the collected video to define specifications for stored video data, including image resolution, frame rate, and retention period, to address specific use, access, and storage requirements.

In contrast, analog-based CCTV systems typically use DVRs for video storage and management, with the analog signal sent directly to the DVR. For long-term storage, many systems employ write-once, read-many media such as optical discs, though these can be cumbersome to manage and lack the recovery capabilities of server-based redundant array of independent disks systems.

The types and quality of connectivity and interfaces required by this CCTV system include both analog and digital communication channels. Traditional analog systems rely on point-to-point cabling, while IP-based systems utilize LANs, WANs, and WLANs, enabling video transmission over vast distances with lower installation costs. The information flows for this physical object include the transmission of video and audio data from cameras to processing and storage systems, as well as communication between cameras, sensors, and other connected devices.

The physical object may be included in the implementation of various systems such as advanced traffic management systems, emergency management systems, and security networks for infrastructure protection. Its applications span traffic monitoring, crime prevention, incident response, and integration with connected and automated vehicles.

Physical Object Device Security Class by Service Package

Although ARC-IT does not specifically address CCTV as a physical object (instead labeling it within an implementation of ITS roadway equipment), two information flows originate from what is assumed to be CCTV: video surveillance coordination and video surveillance control. Table 1 conveys that these information flows appear in 62 service packages. This table also indicates the device security class (1–5) for each information flow 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 related information flows, then go to Table 2 to determine which controls are necessary to protect that physical object as part of the service package. Given a CCTV may be used within multiple service packages, it is necessary to consider the impact of the CCTV on the mission/functions the service package supports, which is addressed by aligning control specifications under the appropriate device security class in Table 2.

Table 1. Physical Object Device Security Class by Service Package

Service Packages	Device Security Class for ITS Roadway Equipment
CVO05: Commercial Vehicle Parking	2
CVO06: Freight Signal Priority	3
CVO10: Road Weather Information for Freight Carriers	2
DM 01: ITS Data Warehouse	2
MC03: Roadway Automated Treatment	3
MC06: Work Zone Management	2
MC07: Work Zone Safety Monitoring	2
MC09: Infrastructure Monitoring	4
MC11: Maintenance and Construction Signal Priority	3
MC12: One-Way Convoy Driving	2
PM04: Regional Parking Management	2
PS03: Emergency Vehicle Preemption	3
PS07: Incident Scene Safety Monitoring	2
PS09: Transportation Infrastructure Protection	5
PS10: Wide-Area Alert	2
PT09: Transit Signal Priority	5
PT10: Intermittent Bus Lanes	2
PT12: Transit Vehicle at Station/Stop Warnings	2
ST01: Emissions Monitoring	2
ST02: Eco-Traffic Signal Timing	3
ST03: Eco-Traffic Metering	2
ST04: Roadside Lighting	2
ST06: HOV/HOT Lane Management	2
ST07: Eco-Lanes Management	2
ST08: Eco-Approach and Departure at Signalized Intersections	3
ST10: Low Emissions Zone Management	2

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

Service Packages	Device Security Class for ITS Roadway Equipment
Traveler Information and Personal Mobility (TI) 07: In-Vehicle Signage	2
TM01: Infrastructure-Based Traffic Surveillance	2
TM03: Traffic Signal Control	3
TM04: Connected Vehicle Traffic Signal System	3
TM05: Traffic Metering	2
TM06: Traffic Information Dissemination	2
TM08: Traffic Incident Management System	2
TM12: Dynamic Roadway Warning	2
TM13: Standard Railroad Grade Crossing	2
TM14: Advanced Railroad Grade Crossing	5
TM15: Railroad Operations Coordination	2
TM16: Reversible Lane Management	4
TM17: Speed Warning and Enforcement	2
TM18: Drawbridge Management	3
TM19: Roadway Closure Management	4
TM20: Variable Speed Limits	2
TM21: Speed Harmonization	2
TM22: Dynamic Lane Management and Shoulder Use	3
TM24: Tunnel Management	5
TM25: Wrong Way Vehicle Detection and Warning	2
TM26: Signal Enforcement	2
Vehicle Safety (VS) 05: Curve Speed Warning	2
VS06: Stop Sign Gap Assist	5
VS07: Road Weather Motorist Alert and Warning	2
VS08: Queue Warning	2

Service Packages	Device Security Class for ITS Roadway Equipment
VS09: Reduced Speed Zone Warning / Lane Closure	2
VS10: Restricted Lane Warnings	2
VS11: Oversize Vehicle Warning	2
VS12: Vulnerable Road User Safety	3
VS13: Intersection Safety Warning and Collision Avoidance	3
VS15: Infrastructure Enhanced Cooperative Adaptive Cruise Control	3
VS16: Automated Vehicle Operations	3
VS17: Management of Electronic Traffic Regulations	3
WX01: Weather Data Collection	3
WX03: Spot Weather Impact Warning	2
WX04: Roadway Micro-Prediction	3

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

Assumptions and Characteristics

This control set document is necessary because ITS physical objects have a set of characteristics and assumptions that differentiate them from other types of technologies (e.g., general enterprise information technology). Figure 1 and Figure 2 illustrate the connectivity and component structure of CCTV systems, providing insight into the rationale behind the selected assumptions. Those assumptions are listed here and are discussed in the following paragraphs:

- Assumption #1: CCTV devices are connected to a secure network.
 - CCTV devices are assumed to be connected to a secure network using protocols such as Transmission Control Protocol (TCP)/IP and Hypertext Transfer Protocol Secure (HTTPS), or a virtual private network (VPN). Additionally, while connecting to a storage device it is assumed that the CCTV architecture is using industry-standard storage protocols such as the Internet Small Computer Systems Interface. They are capable of securely transmitting video data to external services, including video management systems (VMS), monitoring stations, and storage devices. Devices operating in isolated or offline modes may require alternative controls not covered in this set.
- Assumption #2: CCTV is equipped with a trusted power distribution, and the systems operate continuously with minimal downtime.
 - Inadequate power is one of the most common problems with CCTV and could result in total system failure. CCTV systems are assumed to provide surveillance capabilities 24 hours per day,

7 days per week, ensuring real-time monitoring and recording. It is assumed that CCTV systems experience minimal interruptions, which warrants the monitoring of threats to the consistency of CCTV. Continuous operation with minimal interruptions is a key assumption for this control set.

- Assumption #3: CCTV device age and technology are maintained.
 - The control set is designed for modern CCTV systems that are equipped with current communication protocols (e.g., TCP/IP, HTTPS) and are capable of supporting security features like encryption and secure firmware updates. Legacy devices with limited or no support for these technologies are outside the scope of this control set.
- Assumption #4: CCTV systems process both persistent and perishable data.
 - CCTV systems generate both persistent and perishable data. Persistent data, such as archived video footage, requires integrity and confidentiality protection. Perishable data, such as real-time video streams, is often processed and discarded quickly and may not need the same level of protection.
- Assumption #5: CCTV systems are typically deployed in exposed field environments.
 - CCTV systems are often installed outdoors or in remote locations rather than inside buildings. This exposure introduces risks not commonly associated with traditional information technology systems in secure facilities (e.g., traffic management centers [TMCs]). These risks necessitate a focus on physical and environmental (PE) controls tailored to outdoor deployments, such as secure casings, environmental monitoring, and protection against vandalism. Fixed facility Policy and Procedure (PE) controls such as fire suppression systems are typically not applicable to these deployments.
- Assumption #6: CCTV systems include adequate data storage and retention policies.
 - CCTV systems are assumed to be equipped with sufficient storage capacity to accommodate the volume of video data generated during regular operation. This includes the ability to handle high-definition video recordings and maintain archives for extended periods as needed. Additionally, these systems are expected to have well-defined data retention policies that specify how long video data should be stored, procedures for secure deletion when no longer needed, and measures to ensure compliance with relevant regulations and organizational requirements.

Resources for Identifying Threats, Vulnerabilities, and Predisposing Conditions

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

Threat events listed in **Appendix A. Threats, Vulnerabilities, and Predisposing Conditions**, focus on the CCTV, not the larger system comprised of various types of physical objects and other components. Various threat events may ultimately impact CCTV or its mission/operations, either by compromise of the CCTV 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 CCTV can implement a protection measure to mitigate the risk will the threat be considered relevant to the CCTV 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⁽²⁾ controls detailed in chapter 3 and the ITS CSF Profile,⁽⁵⁾ a comprehensive table was developed to map relevant mission objectives for the CCTV system to NIST CSF subcategories, as presented in Table 7. These mission objectives were defined based on the CCTV system's physical and technical attributes, such as surveillance and network connectivity. The following mission objectives were chosen for the CCTV system: #1: Improve physical safety of the transportation ecosystem, #3: Collect, manage, use, and disseminate data, #8: Build privacy protections into ITS operations, and #11: Enhance telecommunications and networking to facilitate emerging ITS capabilities.

Table 7 lists all high-priority NIST CSF subcategories corresponding to these mission objectives, along with carefully selected moderate-priority subcategories relevant to the CCTV system. Using the NIST CSF informative reference tool, appropriate NIST SP 800-53⁽²⁾ controls were identified to address the CCTV 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 CCTV system's unique attributes

Chapter 3. Summary of Control Specifications

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

Table 2 below summarizes the control specifications as they apply in this control set document. The symbols used in the table are as follows:

- “NS” indicates that 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 control², but only to address unique physical object risks and to direct the developer to comply; other parameter values are left to the discretion of the ITS program that is deploying the physical objects to set based on industry practices.
- “R” indicates there is at least one risk reference or resource that informs the control selection.
- “S” indicates there is a standard or practice that the control helps to meet.
- “M” indicates the control is implemented by the manufacturer of the physical object.
- “I” indicates that the control is implemented by the IOO organization.
- “M/I” indicates that the control is implemented by the manufacturer and the IOO organization.

Due to the nature of ITS physical objects and the operational environment, the approach to implement selected controls may need to deviate from that of a typical information technology system ¹ 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 implementation. When this is the case, guidance is provided in chapter 4 of this control set document. The last column of Table 2 indicates if the control should be implemented by the CCTV manufacturer or 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⁽²⁾ 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)

Table 2. Control Specifications by Device Security Class CCTV

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

ID	Title	Device Security Class					Responsibility
		1	2	3	4	5	
AC-6(10)	Prohibit Non-Privileged Users from Executing Privileged Functions	NS	GR	GR	GR	GR	M/I
AC-7	Unsuccessful Logon Attempts	GVR	GVR	GVR	GVR	GVR	M/I
AC-8	System Use Notification	GVR	GVR	GVR	GVR	GVR	M/I
AC-9	Previous Logon Notification	GR	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	GR	GR	GR	GR	GR	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

ID	Title	Device Security Class					Responsibility (Manufacturer (M); IOO (I))
		1	2	3	4	5	
AC-17(6)	Protection of Mechanism Information	G	G	G	G	G	M/I
AC-18	Wireless Access	GR	GR	GR	GR	GR	M/I
AC-18(1)	Authentication and Encryption	GVRs	GVRs	GVRs	GVRs	GVRs	M/I
AC-18(3)	Disable Wireless Networking	G	G	G	G	G	M/I
AC-20	Use of External Systems	GVRs	GVRs	GVRs	GVRs	GVRs	M/I
AC-20(1)	Limits on Authorized Use	G	G	G	G	G	M/I
AC-20(2)	Portable Storage Devices – Restricted Use	GVS	GVS	GVS	GVS	GVS	I
AC-21	Information Sharing	GVR	GVR	GVR	GVR	GVR	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	G	G	G	G	G	M/I
AU-4	Audit Log Storage Capacity	GVR	GVR	GVR	GVR	GVR	M/I
AU-4(1)	Transfer to Alternate Storage	GVR	GVR	GVR	GVR	GVR	M/I
AU-5	Response to Audit Processing Failures	GVR	GVR	GVR	GVR	GVR	M/I

ID	Title	Device Security Class					Responsibility (Manufacturer (M); IOO (I))
		1	2	3	4	5	
AU-5(1)	Storage Capacity Warning	GV	GV	GV	GV	G	M/I
AU-5(2)	Real-Time Alerts	GVR	GVR	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	G	G	G	G	G	I
AU-6(5)	Integrated Analysis of Audit Records	GV	GV	GV	GV	GV	I
AU-6(6)	Correlation with Physical Monitoring	G	G	G	G	G	I
AU-7	Audit Record Reduction and Report Generation	GR	GR	GR	GR	GR	I
AU-9	Protection of Audit Information	NS	GVR	GVR	GVR	GVR	M/I
AU-9(2)	Store on Separate Physical Systems or Components	NS	GVR	GVR	GVR	GVR	M
AU-9(3)	Cryptographic Protection	NS	NS	GRS	GRS	GRS	M
AU-11	Audit Record Retention	GVS	GVS	GVS	GVS	GVS	M/I
AU-12	Audit Record Generation	GVR	GVR	GVR	GVR	GVR	M
AU-12(3)	Audit Record Generation Changes	GVR	GVR	GVR	GVR	GVR	M

ID	Title	Device Security Class					Responsibility (Manufacturer
		1	2	3	4	5	
	By Authorized Individuals						
AU-13	Monitoring for Information Disclosure	GV	GV	GV	GV	GV	I
AU-14	Session Audit	GV	GV	GV	GV	GV	M/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	G	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(6)	Automation Support for Monitoring	GV	GV	GV	GV	GV	M/I
CA-8	Penetration Testing	GVR	GVR	GVR	GVR	GVR	I
CA-9	Internal System Connections	GVR	GVR	GVR	GVR	GVR	M/I
CA-9(1)	Compliance Checks	G	G	G	G	G	I
CM-2	Baseline Configuration	G	G	G	G	G	I
CM-3	Configuration Change Control	GVR	GVR	GVR	GVR	GVR	M/I

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

ID	Title	Device Security Class					Responsibility (Manufacturer (M); IOO (I))
		1	2	3	4	5	
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	NS	GV	GV	GV	GV	I
CM-6	Least Functionality 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	GVR	GVR	GVR	GVR	GVR	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-8(1)	Updates During Installation and Removal	G	G	G	G	G	I
CM-9	Configuration Management Plan	GV	GV	GV	GV	GV	I
CM-11	User-Installed Software	GVR	GVR	GVR	GVR	GVR	M/I
CM-11(2)	Software Installation with Privileged Status	G	G	G	G	G	M/I

ID	Title	Device Security Class					Responsibility (Manufacturer (M); IOO (I))
		1	2	3	4	5	
CM-12	Information Location	GR	GR	GR	GR	GR	I
CM-13	Data Action Mapping	G	G	G	G	G	I
CM-14	Signed Components	GR	GR	GR	GR	GR	M/I
CP-6	Alternate Storage Site	G	G	G	G	G	I
CP-7	Alternate Processing Site	GVR	GVR	GVR	GVR	GVR	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-10	System Recovery and Reconstitution	GVR	GVR	GVR	GVR	GVR	M/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	GR	GR	GR	GR	GR	I
IA-3	Device Identification and Authentication	GVR	GVR	GVR	GVR	GVR	M/I
IA-4	Identifier Management	GV	GV	GV	GV	GV	M/I
IA-5	Authenticator Management	GVRs	GVRs	GVRs	GVRs	GVRs	M/I

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

ID	Title	Device Security Class					Responsibility (Manufacturer (M); IOO (I))
		1	2	3	4	5	
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
MP-2	Media Access	GV	GV	GV	GV	GV	I
MP-3	Media Marking	GVR	GVR	GVR	GVR	GVR	I
MP-4	Media Storage	GV	GV	GV	GV	GV	M/I
MP-4(2)	Automated Restricted Access	GV	GV	GV	GV	GV	M/I
MP-7	Media Use	GVR	GVR	GVR	GVR	GVR	M/I
MP-8	Media Downgrading	GV	GV	GV	GV	GV	I
PE-2	Physical Access Authorizations	GV	GV	GV	GV	GV	I
PE-2(1)	Access by Position or Role	G	G	G	G	G	I
PE-3	Physical Access Control	GVR	GVR	GVR	GVR	GVR	M/I
PE-3(1)	System Access	GV	GV	GV	GV	GV	I
PE-3(4)	Lockable Casings	GV	GV	GV	GV	GV	M/I
PE-3(5)	Tamper Protection	GV	GV	GV	GV	GV	M/I
PE-4	Access Control for Transmission	GVR	GVR	GVR	GVR	GVR	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

ID	Title	Device Security Class					Responsibility
		1	2	3	4	5	
PE-11	Emergency Power	GV	GV	GV	GV	GV	M/I
PE-14	Environmental Controls	GVR	GVR	GVR	GVR	GVR	M/I
PE-14(2)	Environmental Controls Monitoring with Alarms and Notifications	GV	GV	GV	GV	GV	M/I
PE-21	Electromagnetic Pulse Protection	GVR	GVR	GVR	GVR	GVR	M/I
PL-2	System Security and Privacy Plans	GVR	GVR	GVR	GVR	GVR	I
PL-7	Concept of Operations	GVR	GVR	GVR	GVR	GVR	I
PL-8	Security and Privacy Architectures	GV	GV	GV	GV	GV	I
PM-5	System Inventory	GV	GV	GV	GV	GV	M/I
PM-9	Risk Management Strategy	GVS	GVS	GVS	GVS	GVS	M/I
PM-30	Supply Chain Risk Management Strategy	GV	GV	GV	GV	GV	M/I
PM-30(1)	Suppliers of Critical or Mission-Essential Items	G	G	G	G	G	M/I
PS-3	Personnel Screening	GV	GV	GV	GV	GV	I
PS-4	Personnel Termination	GV	GV	GV	GV	GV	I

ID	Title	Device Security Class					Responsibility (Manufacturer (M); IOO (I))
		1	2	3	4	5	
PS-6	Access Agreements	GV	GV	GV	GV	GV	I
RA-3	Risk Assessment	GV	GV	GV	GV	GV	M/I
RA-3(1)	Risk Assessment Supply Chain Risk Assessment	G	G	G	G	G	I
RA-5	Vulnerability Scanning	GR	GR	GR	GR	GR	M/I
RA-5(6)	Vulnerability Scanning Automated Trend Analysis	G	G	G	G	G	I
RA-8	Privacy Impact Assessments	G	G	G	G	G	M/I
SA-4	Acquisition Process	GR	GR	GR	GR	GR	M/I
SA-4(2)	Acquisition Process Design and Implementation Information for Controls	GVR	GVR	GVR	GVR	GVR	M/I
SA-4(5)	Acquisition Process System, Component, and Service Configuration	GV	GV	GV	GV	GV	M/I
SA-4(9)	Acquisition Process 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

ID	Title	Device Security Class					Responsibility (Manufacturer (M); IOO (I))
		1	2	3	4	5	
SA-9	External System Services	GV	GV	GV	GV	GV	I
SA-9(2)	External System Services Identification of Functions, Ports, Protocols, and Services	GV	GV	GV	GV	GV	I
SA-10	Developer Configuration Management	GVR	GVR	GVR	GVR	GVR	I
SA-10(1)	Developer Configuration Management Software and Firmware Integrity Verification	GR	GR	GR	GR	GR	M/I
SA-10(3)	Developer Configuration Management 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)	Developer Security Testing and Evaluation Threat Modeling and Vulnerability Analyses	GV	GV	GV	GV	GV	M/I
SA-11(6)	Developer Security Testing and Evaluation Attack Surface Reviews	G	G	G	G	G	M/I

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/I
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	G	G	G	G	G	M
SC-4	Information In Shared Resources	GR	GR	GR	GR	GR	M
SC-5	Denial-of-Service Protection	GVR	GVR	GVR	GVR	GVR	M/I

ID	Title	Device Security Class					Responsibility (Manufacturer (M); IOO (I))
		1	2	3	4	5	
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
SC-5(3)	Denial-of-Service Protection Detection and Monitoring	GV	GV	GV	GV	GV	M/I
SC-6	Resource Availability	G	G	G	G	G	M
SC-7	Boundary Protection	GVR	GVR	GVR	GVR	GVR	I
SC-7(3)	Boundary Protection Access Points	GR	GR	GR	GR	GR	I
SC-7(5)	Boundary Protection Deny by Default — Allow by Exception	GVR	GVR	GVR	GVR	GVR	I
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(15)	Boundary Protection Networked Privileged Access	G	G	G	G	G	M/I

ID	Title	Device Security Class					Responsibility (Manufacturer (M); IOO (I))
		1	2	3	4	5	
SC-7(16)	Boundary Protection Prevent Discovery of System Components	G	G	G	G	G	M
SC-7(19)	Boundary Protection Block Communication from Non-Organizationally Configured Hosts	GV	GV	GV	GV	GV	M/I
SC-7(20)	Boundary Protection Dynamic Isolation and Segregation	GVR	GVR	GVR	GVR	GVR	M/I
SC-7(21)	Boundary Protection Isolation of System Components	GVR	GVR	GVR	GVR	GVR	M
SC-7(24)	Boundary Protection Personally Identifiable Information	GVS	GVS	GVS	GVS	GVS	M/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	GVRS	GVRS	GVRS	GVRS	GVRS	M
SC-10	Network Disconnect	GVR	GVR	GVR	GVR	GVR	M
SC-11	Trusted Path	GV	GV	GV	GV	GV	M
SC-13	Cryptographic Protection	GRS	GRS	GRS	GRS	GRS	M

ID	Title	Device Security Class					Responsibility (Manufacturer (M); IOO (I))
		1	2	3	4	5	
SC-16	Transmission of Security and Privacy Attributes	GV	GV	GV	GV	GV	M/I
SC-17	Public Key Infrastructure Certificates	GV	GV	GV	GV	GV	M/I
SC-23	Session Authenticity	GRS	GRS	GRS	GRS	GRS	M/I
SC-23(1)	Session Authenticity Invalidate Session Identifiers at Logout	G	G	G	G	G	M
SC-28	Protection of Information at Rest	GVR	GVR	GVR	GVR	GVR	M
SC-28(1)	Protection of Information at Rest Cryptographic Protection	GV	GV	GV	GV	GV	M
SC-28(3)	Protection of Information at Rest Cryptographic Keys	GVS	GVS	GVS	GVS	GVS	M
SC-32	System Partitioning	GVR	GVR	GVR	GVR	GVR	M/I
SC-35	External Malicious Code Identification	G	G	G	G	G	M
SC-36	Distributed Processing and Storage	NS	NS	NS	GV	GV	M/I
SC-39	Process Isolation	NS	NS	GR	GR	GR	M
SC-39(1)	Hardware Separation	NS	NS	G	G	G	M
SC-40	Wireless Link Protection	GVS	GVS	GVS	GVS	GVS	M

ID	Title	Device Security Class					Responsibility (Manufacturer (M); IOO (I))
		1	2	3	4	5	
SC-41	Port and I/O Device Access	GVR	GVR	GVR	GVR	GVR	M/I
SC-43	Usage Restrictions	NS	GVS	GVS	GVS	GVS	M/I
SC-49	Hardware-Enforced Separation and Policy Enforcement	NS	NS	GV	GV	GV	M/I
SC-51	Hardware-Based Protection	NS	NS	GVR	GVR	GVR	M
SI-2	Flaw Remediation	GVR	GVR	GVR	GVR	GVR	M/I
SI-3	Malicious Code Protection	GVR	GVR	GVR	GVR	GVR	M/I
SI-3(4)	Malicious Code Protection Updates Only by Privileged Users	G	G	G	G	G	M/I
SI-4	System Monitoring	GVRs	GVRs	GVRs	GVRs	GVRs	M/I
SI-4(4)	System Monitoring Inbound and Outbound Communication Traffic	GVR	GVR	GVVR	GR	GVR	M/I
SI-4(7)	System Monitoring Automated Response to Suspicious Events	GV	GV	GV	GV	GV	M/I
SI-4(14)	System Monitoring Wireless Intrusion Detection	G	G	G	G	G	M/I
SI-7	Software, Firmware, and Information Integrity	GVR	GVR	GVR	GVR	GVR	M/I
SI-7(1)	Software, Firmware, and Information	GVR	GVR	GVR	GVR	GVR	M/I

ID	Title	Device Security Class					Responsibility (Manufacturer (M); IOO (I))
		1	2	3	4	5	
	Integrity Integrity Checks						
SI-7(2)	Software, Firmware, and Information Integrity Automated Notifications of Integrity Violations	GVR	GVR	GVR	GVR	GVR	M/I
SI-10	Information Input Validation	GVR	GVR	GVR	GVR	GVR	M/I
SI-16	Memory Protection	GVR	GVR	GVR	GVR	GVR	M
SR-2	Supply Chain Risk Management Plan	GV	GV	GV	GV	GV	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	GR	GR	GR	GR	GR	M/I
SR-10	Inspection of Systems or Components	G	G	G	G	G	M/I
SR-12	Component Disposal	GV	GV	GV	GV	GV	I

Chapter 4. Detailed Control Specifications

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

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

- Various aspects of a control may be implemented by different roles, depending on whether the control content is technical, non-technical, or a combination of both. Non-technical controls (e.g., policies, procedures, desired security functionality, leadership/management decisions) are most often implemented by the IOO. Within the IOO there may be ITS engineers/integrators (organic or contracted) who manage some of the non-technical security decisions, but more likely manage the bulk of the technical security decisions on behalf of the IOO leadership/management. Technical controls are typically implemented by the system and, therefore, would be levied against a developer (organic or contracted) or a manufacturer/vendor. However, the IOO must often make decisions on the technical aspects of the system and convey those to the manufacturer/vendor for design and implementation. Therefore, some controls are tagged herein as M/I regardless of whether they are tagged in NIST SP 800-53(2) 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 a CCTV (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 is 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 CCTV. In some cases, the guidance for the selected controls and control enhancements must be modified from NIST SP 800-53(2) to address the characteristics of the topic of the control set and the environments in which the system or components operate.

Parameter Value(s) (PVs): The control text in NIST SP 800-53(2) 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 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 CCTV within the scope of this control set, no parameter value entry is included. Organizations within the ITS community must define all remaining parameter values for controls selected for systems within their organization.

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

- For example, “#2” indicates the value being provided 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 the paragraph or subparagraph, and annotation of its placement 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(2) to fully understand the meaning.

Risk References and Resources: If there is an authoritative source (e.g., ATT&CK for ICS,⁽⁷⁾ NIST SP 800-82,⁽⁴⁾ or ARC-IT⁽⁶⁾) 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 CCTV implementation are listed, as not every technique is feasible or possible against a typical CCTV. 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(4) includes an “OT Discussion” for some controls in its overlay for operational technology (OT). Those discussions are included if relevant to the CCTV, but wording may be adapted to the unique features or functions of the CCTV.
- The ARC-IT Mechanisms are requirements-like statements that could be conveyed to a manufacturer/vendor for CCTV design and implementation.

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

Guidance: This is an organizational control, as the IOO (not the manufacturer) would create policies and procedures. If the IOO does not have access control policies and procedures, the integrator, engineers, or developers may not have adequate guidance to design, develop, and manage access control capabilities in the CCTV. This control is not implemented on or by the CCTV itself; the IOO develops, publishes, and conveys to the manufacturer/vendor access control policies and procedures to guide implementation of other access controls from this family on the CCTV.

Parameter Value(s):

paragraph a. “CISO or equivalent cybersecurity authority; IT/OT security administrators; traffic operations management; CCTV system administrators; and other personnel or roles with access control responsibilities.””

paragraph a.1. “System-level”

paragraph b “CISO, Chief Information Security Officer designee, or other IOO-designated official responsible for cybersecurity governance.”

paragraph c.1. #1 “at least annually”

paragraph c.1. #2 “Device or vendor onboarding; security incidents or suspected compromises; intrusion detections; significant changes to CCTV system architecture or configuration; or changes to the applicable CCTV control set.”

paragraph c.2. #1 at least annually”

paragraph c.2. #2 “Device or vendor onboarding; security incidents or suspected compromises; intrusion detections; significant changes to CCTV system architecture or configuration; or changes to the applicable CCTV control set.”

Risk References and Resources:

NIST SP 800-82⁽⁴⁾: 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): M/I

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

Guidance: The IOO is responsible for defining and managing account policies and processes, while the manufacturer or vendor is responsible for providing account management capabilities within the CCTV device and associated video management systems. Account management is fundamental to protecting access to CCTV; poorly protected accounts may have direct access to the VMS, potentially impacting the confidentiality, integrity, and availability of recently captured video.

Each camera and VMS must use unique administrator credentials and role-based accounts with least privilege. Disable default usernames, enforce minimum 12-character passwords or X.509 cert-based logins, and lock accounts after five failed attempts for 15 minutes.

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, operational control, administrative access to video management and storage functions)"

paragraph f. "Account Management Policy"

paragraph h. "Security administrators, CCTV system administrators, human resources, or other designated personnel or roles."

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⁽⁴⁾: In ITS systems, physical security, personnel security, intrusion detection, or auditing measures may support this control objective.

ARC-IT Mechanisms:

- The device will automatically terminate a user's session after a reasonably short period of time consistent with industry practices and the sensitivity of the user's session. In most cases 5–15 minutes is reasonable.

- 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 that information system data integrity is preserved during system maintenance.
- The organization will employ a wide range of heuristics to monitor and report 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, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: This control requires the IOO to manage accounts, including disabling accounts after a defined period under the conditions discussed in the control text. The manufacturer or vendor provides the technical capability to disable or suspend accounts within the CCTV device, video management system, or associated authentication services. Where device limitations exist, network-based or procedural compensating controls may be used.

Parameter Value(s):

#1 “72 hours of account inactivity or following expiration of authorized access.”

paragraph d. “90 days”

Risk References and Resources:

NIST SP 800-82⁽⁴⁾: When the ITS (e.g., field devices) cannot support temporary or emergency accounts, this enhancement does not apply. Examples of compensating controls include employing non-automated mechanisms or procedures.

Standards: NIST SP 800-82⁽⁴⁾

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: This control requires automated auditing of account management actions such as account creation, modification, disabling, and removal. For CCTV deployments, these actions are typically performed within centralized video management systems, authentication services, or supporting operating systems rather than directly on individual cameras. The manufacturer or vendor provides the capability to generate audit records for account management actions, while the IOO ensures that such events are selected, reviewed, and retained in accordance with AU-2 and related audit controls. Where CCTV devices do not support automated auditing of account actions, compensating controls may be applied at supporting systems.

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

Responsible Party (M/I): M/I

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

Guidance: The Infrastructure Owner and Operator (IOO) define the expected inactivity period or circumstances under which users must log out of CCTV interfaces. This control establishes policy expectations and user responsibilities; automated session termination is addressed separately under AC-11 (Device Lock). The manufacturer/vendor supports this control by ensuring that all CCTV user interfaces (local console, web UI, or management API) provide a clear and accessible logout capability so the IOO’s policy can be implemented effectively.

Parameter Value(s):

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

Risk References and Frameworks:

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⁽⁴⁾

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: In modern transportation CCTV deployments, access enforcement is implemented across a coordinated set of components, including the CCTV device, associated video management systems (VMS), management interfaces, and supporting network infrastructure. Access requests are permitted or denied in accordance with IOO-defined access control policies that consider authenticated identity, assigned roles or privileges, and authorized CCTV functions.

Parameter Value(s):

“authenticated identity, assigned role/privilege level, and requested CCTV function (e.g., live view, playback, export, Pan-Tile-Zoom (PTZ) control, configuration, maintenance)”

Risk References and Resources:

NIST SP 800-82⁽⁴⁾: The organization ensures access enforcement mechanisms do not adversely impact the operational performance of the ITS. Example of 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

ARC-IT Mechanisms:

- The device should support a role-based access mechanism in which:
 - There is an access control policy that defines protected resources and functions to which access control is applied; users and processes must demonstrate that they are authorized to access those resources according to the policy.
 - The device should be able to grant at least one of ongoing privileged access or periodic privileged access as defined in Notes on Access Control.⁽¹³⁾
 - The device may support an installer that can grant ongoing privileged access to installed processes.
 - The access control policy may only be edited by privileged users.

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

Responsible Party (M/I): M/I

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

Guidance: The IOO should implement dual authorization for defined high-risk or high-impact access activities involving the VMS or associated video storage systems (e.g., NAS, SAN), where unauthorized actions could affect system integrity, availability, or evidentiary value of video data.

Parameter Value(s):

"Remote administrative access from the TMC; camera configuration changes; modifications to video feeds or recording settings; read/write access to the video management system or associated network-attached storage; pan-tilt-zoom (PTZ) control functions."

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

Responsible Party (M/I): M/I

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

Guidance: The IOO should define discretionary access control policies that allow authorized personnel to grant, modify, or revoke access to CCTV resources in accordance with organizational policy. The IOO should develop and maintain user training to ensure discretionary permissions are applied appropriately and reviewed as needed. The manufacturer or vendor should provide functionality within the CCTV system, video management system (VMS), or associated management interfaces to support discretionary access control, including the ability to centrally manage and modify permissions in support of TMC operations.

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 of 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. But it may not provide sufficient granularity when users need 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).

Guidance: The IOO should establish information flow control policies to ensure that the exchange of information between systems is securely managed. Manufacturers and vendors should implement any connection to the CCTV firewall in a manner that enforces secure information flow between

systems connected to the VMS, the NAS, or any external information flows in compliance with the established policies.

Parameter Value(s):

“segmentation policies that restrict video and control data flows to authorized monitoring stations and prohibit unauthorized outbound information flows from CCTV devices to external networks.”

Risk References and Resources:

ATT&CK for ICS Mitigations / Techniques:

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

NIST SP 800-82⁽⁴⁾: 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).

ARC-IT Mechanisms:

- The device should support defining information flow control policies which identify constraints on the flow of information in and out of the device, including in particular IA and SC mechanisms that must be applied to information flows for them to be permissible. See Notes on Access Control⁽¹³⁾ for a discussion and examples of information flow control.
- The ability to define an information flow control policy should be restricted to privileged users.

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

Responsible Party (M/I): M/I

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

Guidance: The IOO should define policies governing the use of encryption for CCTV video and control information transmitted between system components and external systems. Manufacturers and vendors should implement mechanisms that ensure encrypted information flows are permitted, restricted, or blocked in accordance with IOO-defined policies, including for connections between CCTV devices, video management systems, storage systems, and external networks.

Parameter Value(s):

#1 “encryption-aware flow control mechanisms that permit or restrict encrypted video and control traffic based on approved endpoints, protocols, certificates, or communication paths.”

AC-5, Separation of Duties

Responsible Party (M/I): M/I

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

Guidance: The IOO should define separation-of-duties requirements for sensitive CCTV operational and administrative functions. The manufacturer or vendor should provide role-based capabilities within the CCTV device, camera controller, and video management system to support enforcement of these separations. Distinct roles should be established for activities such as video monitoring, camera control, system configuration, and access control administration to reduce the risk of misuse or unauthorized modification.

Parameter Value(s):

"Separation between roles responsible for live video monitoring, camera hardware or firmware maintenance, video management system configuration, and approval or handling of video access or release requests."

Risk References and Resources:

NIST SP 800-82⁽⁴⁾: Example compensating controls include providing increased personnel security and auditing.

AC-6, Least Privilege

Responsible Party (M/I): M/I

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

Guidance: The IOO should implement the principle of least privilege to restrict access rights to the minimum necessary to perform assigned tasks. For example, CCTV technicians may be limited to maintenance and diagnostic functions such as configuration updates or log retrieval, while administrative privileges for system-wide changes, software updates, or access control configuration are restricted to designated administrators. This minimizes risks of unauthorized access, privilege escalation, and system misuse.

Risk References and Resources:

ATT&CK for ICS Mitigations / Techniques:

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

NIST SP 800-82⁽⁴⁾: 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).

ARC-IT Mechanisms: See AC-3.

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.

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

Guidance: The IOO should define the individuals and roles that require access to security functions, identify which security functions are implemented in hardware, software, and firmware, and specify the security-relevant information that requires authorized access. Manufacturers and vendors are expected to provide authorization mechanisms within CCTV devices, video management systems, and supporting components that enable enforcement of these least-privilege requirements.

Parameter Value(s):

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

paragraph a. "Physically access the system console or camera network interface for device commissioning, configuration, diagnostics, and verification of firmware integrity

paragraph b **"(for Local Administrators, Field Technicians, and Remote Administrators)** manage camera firmware versions, configuration settings, configuration logs, audit logs, device certificates, and network configuration data;

(for Remote Administrators) manage certificates, cryptographic keys, and user access permissions for centralized video management systems (VMS), configure network interfaces and encryption settings, and review and archive system and security event logs;

(for Vendors) verify firmware signatures, perform system integrity validation, and provide authenticated software updates."

Risk References and Resources:

NIST SP 800-82⁽⁴⁾: 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 Privilege Commands

Responsible Party (M/I): M/I

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

Guidance: The IOO should define the privileged commands relevant to the services offered by the VMS and the NAS for which there are compelling operational needs requiring authorized access to the CCTV via network access. These should be documented in the security plan for the system.

Parameter Value(s):

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

#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⁽⁴⁾: In situations where the ITS components (e.g., CCTV) 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/I

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

Guidance: This control ensures that CCTV software components—both system-level and application-level—execute only with the minimum privileges necessary for their intended function. Manufacturers implement this by designing CCTV operating systems, containers, and application frameworks so that:

- Each software process runs under a dedicated service or system account with limited access rights;
- Code modules cannot escalate to administrative or root privileges except through an explicitly authorized, auditable mechanism (e.g., signed update or secure boot process); and
- Development and integration toolchains enforce principles of least privilege during build, deployment, and runtime (e.g., sandboxing, SELinux profiles, capability bounding, or container security contexts).

Parameter Value(s): “CCTV operating-system services, middleware, and application modules execute only with the privileges associated with their assigned service or user context; execution with root or administrative privileges is restricted to 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: The IOO should create a list of privileged functions or request a list from the manufacturer/vendor. The manufacturer/vendor should implement the functionality to prevent non-privileged users from executing those functions as required by policy.

Risk References and Resources:

NIST SP 800-82⁽⁴⁾: Example compensating controls include enhanced auditing.

ARC-IT Mechanisms: See AC-06.

AC-7, Unsuccessful Logon Attempts

Responsible Party (M/I): M/I

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

Guidance: The IOO should define the number of consecutive invalid logon attempts to CCTV control software and the time period for tracking these attempts, as well as specify automated actions (e.g., account lockout, administrator notification, or logon delay) to be triggered when the limit is exceeded. The manufacturer/vendor should implement these unsuccessful logon attempt requirements in the CCTV control software, ensuring that the system enforces the IOO-defined policy, including support

for disconnected operations where no connection to the centralized VMS exists, such as by locally locking the camera controller after the specified number of failed attempts to prevent unauthorized access to video feeds or camera controls.

Parameter Value(s):

paragraph a. #1 "5"

paragraph a. #2 "15 minutes"

paragraph b. "Lock the account or node until released by an administrator; notify system administrator"

Risk References and Resources:

NIST SP 800-82⁽⁴⁾: 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 logons of 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

ARC-IT Mechanisms:

- The device supports the functionality of defining what types of authentication attempts should be counted for the purposes of further security action.
- The device should support login as one of these types of authentication attempts and may support other types of authentication attempts, for example authentication attempts for specific types of access to specific resources.
- The device should support counting unsuccessful authentication attempts for users and locking them out for a period of time.
- The device is configurable such that for accounts with identified privileged roles the threshold number of unsuccessful login attempts is three in 5 minutes, and the lockout period is 5 minutes starting immediately after the third unsuccessful login attempt.
- The device may be configurable in such that a user's role exists that allows a user in that role to unlock other user's accounts before the lockout period expires.
- This feature should not reveal valid users of the system through the invalid login error messages it gives. Generic error messages should be provided that do not reveal valid user information.
- The authentication system response time should not noticeably different for valid and invalid users.

AC-8, System Use Notification

Responsible Party (M/I): M/I

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

Guidance: The IOO should define system use notification requirements for administrative and operational access to CCTV systems. Manufacturers and vendors should implement system use notifications on CCTV devices, video management systems (VMS), and associated management interfaces so that users are informed of authorized use, monitoring, and restrictions prior to or upon interactive access. Where direct notification is not technically feasible, compensating mechanisms may be used in accordance with organizational policy.

Parameter Value(s):

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

Risk References and Resources:

NIST SP 800-82⁽⁴⁾: Many ITS systems must remain in continuous operation, and system use notification may not be supported or effective. Example of compensating controls include posting physical notices in ITS facilities or providing recurring training on system use prior to permitting access.

ARC-IT Mechanisms: Exactly as specified in control.

AC-9, Previous Logon Notification

Responsible Party (M/I): I

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

Guidance: The IOO should define procedures for responding to suspicious activity identified through previous logon notifications. Manufacturers and vendors should provide the capability for CCTV devices or management interfaces to display information about the previous successful and unsuccessful logon attempts to users upon login, supporting user awareness and timely reporting of potential unauthorized access.

Risk References and Resources:

ATT&CK for ICS Mitigations / Techniques:

- M0919 / T0863

AC-10, Concurrent Session Control

Responsible Party (M/I): M/I

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

Guidance: The IOO should specify the maximum number of concurrent sessions permitted for each CCTV account type (e.g., operator, administrator) to reduce the risk of unauthorized or uncontrolled access to video feeds and management functions. Manufacturers and vendors are expected to provide CCTV control software that enforces these limits, including during disconnected operations.

Parameter Value(s):

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

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

Risk References and Resources:

NIST SP 800-82⁽⁴⁾: The number, account type, and privileges of concurrent sessions consider the roles and responsibilities of the affected individuals. Example of 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 CCTV 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 CCTV when an operational user logs in but leaves the system accessible when no longer using the CCTV.

Guidance: The IOO should determine the policy for locking CCTV components. Manufacturers and vendors are expected to provide capabilities that (1) automatically lock the component after a period of user inactivity based on IOO policy and (2) allow users to manually initiate a device lock. Locking in a user session should not prevent other authorized users from logging in or interfering with normal system operation.

Parameter Value(s):

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

Risk References and Resources:

ATT&CK for ICS Mitigations / Techniques:

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

NIST SP 800-82⁽⁴⁾: 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.

ARC-IT Mechanisms:

- The device supports the functionality of monitoring user activity for users in privileged roles and locking out the session after a certain period of inactivity, such that the user must re-authenticate to continue carrying out privileged activities.

- The device is configurable such that the threshold inactivity length is 5 minutes.
- The device supports the functionality of an appropriately privileged user being able to explicitly lock an active session at any time.
- The device should support the functionality of a user locking their own session.
- The device may support the functionality of an appropriately privileged administrator for locking in another user's session.

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: The IOO should define user session termination conditions and trigger events requiring session disconnection for CCTV devices, video management systems (VMS), and associated management interfaces. Manufacturers and vendors are expected to provide capabilities within CCTV components to support enforcement of IOO-defined session termination policies.

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:

ATT&CK for ICS Mitigations / Techniques:

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

NIST SP 800-82⁽⁴⁾: Example compensating controls include providing increased auditing measures or limiting remote access privileges to key personnel.

ARC-IT Mechanisms:

- The device supports the functionality of an appropriately privileged user being able to terminate an active session at any time.
- The device should support the functionality of a user terminating their own session.
- The device may support the functionality of an appropriately privileged administrator terminating another user's session.
- The device should display an explicit logout message to users indicating the reliable termination of authenticated communications sessions.

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

Responsible Party (M/I): M

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

Guidance: The manufacturer or vendor should implement a logout capability for all authenticated CCTV interfaces to allow users to voluntarily terminate their sessions. The logout capability should immediately invalidate the user's active session or authentication token to reduce the risk of session

hijacking or reuse. Logout functionality should be available on all interfaces that support user authentication, including the local console, web-based configuration portals, and remote management interfaces such as SSH.

Parameter Value(s):

“User-initiated logout capability on all authenticated CCTV interfaces (e.g., local console, web UI, SSH) that immediately terminates the session and invalidates 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).

Guidance: The IOO should identify and document in the system security plan specific user actions, such as viewing public-facing CCTV feeds (e.g., traffic webcams), that may be performed without identification or authentication, consistent with public information-sharing missions. Manufacturers and vendors are expected to provide CCTV control software capabilities that allow these actions to be performed without logon, while ensuring that sensitive functions such as camera control, configuration, or feed management require authentication. The IOO must justify these actions in the system security plan and ensure that no other actions bypass identification or authentication unless explicitly authorized.

Parameter Value(s):

“Unauthenticated access limited to viewing designated public-facing CCTV video streams; no control, configuration, recording, playback, export, or administrative functions permitted without identification or authentication.”

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 should define security attributes (e.g., data sensitivity, access restrictions) and privacy attributes (e.g., personally identifiable information [PII] handling for video feeds) for CCTV information and document these in the system security plan, including permitted values and change control requirements. Manufacturers and vendors are expected to provide mechanisms in CCTV control software that support binding these attributes to information during storage, processing, and transmission to enable secure access and information flow enforcement.

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, Moderate}; {24 hours, 30 days, 1 year, IOO-defined}; {Operator, Administrator, Vendor, Maintenance}; {Yes, No}; {IOO-approved cryptographic protection level}

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

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

paragraph d. "Classification levels, sensitivity ratings, cryptographic protections, and retention periods are constrained by IOO-defined policies and applicable legal, regulatory, and privacy requirements for ITS data."

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

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

Standards: ISO 27002:2022⁽²⁷⁾ Control 5.12 - Classification of Information; ISO 27002:2022⁽²⁷⁾ Control 5.13 - Labelling of Information; FIPS 199⁽²⁸⁾; FIPS 140-3⁽¹⁸⁾

AC-17, Remote Access

Responsible Party (M/I): I

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

Guidance: This control applies to both the IOO and the manufacturer or vendor. The IOO defines policies and conditions under which remote access to CCTV systems is permitted, including access to CCTV devices, video management systems (VMS), storage systems, and associated management interfaces. These policies specify authorized users, approved timeframes, authentication requirements, and permitted remote activities. Manufacturers and vendors are expected to provide remote access capabilities that support enforcement of these policies using secure, encrypted communication mechanisms, with appropriate authentication, session control, and logging. Remote access should be restricted to organization-approved operational or maintenance windows and monitored in accordance with AC-17(1).

Risk References and Resources:

ATT&CK for ICS Mitigations / Techniques: M0935 / T0822

NIST SP 800-82⁽⁴⁾: 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.

ARC-IT Mechanisms: See SC-8, SC-12, SC-13.

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 should define monitoring and control requirements for all remote access sessions to CCTV devices, video management systems (VMS), storage systems, and associated management interfaces. Manufacturers and vendors are expected to provide capabilities that record and support monitoring of remote access session initiation, duration, and termination, including user identity, access method, and target system. These capabilities support detection of unauthorized or anomalous remote access activity and enable enforcement of IOO-defined remote access controls.

Risk References and Resources:

NIST SP 800-82⁽⁴⁾: 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: Manufacturers and vendors are expected to ensure that all remote access sessions to CCTV devices, video management systems (VMS), storage systems, and associated management interfaces are protected to maintain the confidentiality and integrity of transmitted information. Remote access communications should employ strong, mutually authenticated encryption mechanisms consistent with organizational policy and applicable standards, protecting video data, credentials, and management commands from interception or modification during remote access.

Risk References and Resources:

NIST SP 800-82⁽⁴⁾: 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.

Standards: Request for Comment (RFC) 8446 Internet Engineering Task Force (IETF), Transport Layer Security (TLS) Protocol Version 1.3, August 2018⁽¹⁴⁾.

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

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 should define which remote access mechanism information is considered sensitive, such as configuration details, authentication methods, credentials, cryptographic material, endpoint identifiers, or connection parameters, and specify which roles are authorized to access this information. Manufacturers and vendors are expected to provide mechanisms within CCTV devices,

video management systems (VMSMS), storage systems, and associated management interfaces to restrict access to remote access mechanism information and protect it from unauthorized disclosure.

AC-18, Wireless Access

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, and threat event “Install general-purpose sniffers on organization-controlled information systems or networks” in table 3, Deliver/Insert/Install Malicious Capabilities.

Guidance: This control is selected to ensure that the IOO explicitly defines whether wireless access is permitted, restricted, or prohibited for CCTV systems. Modern transportation of CCTV devices and supporting components may include wireless capabilities (e.g., cellular, Wi-Fi, Bluetooth, or other radios) that are enabled by default or used for installation, maintenance, or backhaul connectivity. The IOO should establish policy governing the use of wireless technologies, including approved use cases, access restrictions, and configuration controls, or explicitly require that wireless capabilities be disabled when not operationally required. Manufacturers and vendors are expected to provide the capability to disable, restrict, and securely configure wireless interfaces in accordance with IOO-defined policy.

Risk References and Resources:

NIST SP 800-82⁽⁴⁾: 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-1, AC-3, AC-6

- Only highly privileged users explicitly identified will have permission to modify wireless configurations. See AC-3.
- Organizations should conduct periodic wireless site surveys to look for rogue wireless networking devices and to measure physical areas where the wireless communication might be accessible from outside the physical constraints of the building.
- 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: This control is both organizational and technical. The IOO defines requirements for authentication and encryption of any wireless access used by the CCTV system, including which users or devices may access wireless interfaces and under what conditions. Manufacturers and vendors are expected to provide CCTV systems that support strong authentication and encryption for wireless communications, consistent with organizational policy and applicable standards (e.g., WPA3-Enterprise for Wi-Fi-based wireless access, where applicable), and that allow wireless interfaces to be disabled or restricted when not operationally required.

Parameter Value(s):

“Users and devices authorized to authenticate to wireless interfaces.”

Risk References and Resources:

NIST SP 800-82⁽⁴⁾: 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.

Standards: National Transportation Communications for ITS Protocol (NTCIP) 9014 v01.20, Annex B⁽¹⁵⁾

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

Responsible Party (M/I): M/I

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

Guidance: The IOO should determine whether wireless networking is required for CCTV operations and explicitly document approved or prohibited use of wireless interfaces in the system security plan. Where wireless networking is not required, the IOO should require that wireless interfaces be disabled. Manufacturers and vendors are expected to provide the capability to disable, remove, or permanently deactivate wireless networking functions (e.g., Wi-Fi, Bluetooth, cellular radios) through configuration, firmware settings, or physical means, and to prevent re-enablement by unauthorized users.

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: This control applies to the use of systems that are external to the defined CCTV system boundary, such as vendor maintenance systems, contractor laptops, jump hosts, business IT systems, or personally owned devices. The IOO should establish rules governing whether and how such external systems may access CCTV devices, video management systems (VMS), storage systems, or associated management interfaces, including permitted functions, security requirements, and monitoring expectations. Manufacturers and vendors are expected to provide capabilities that support enforcement of these restrictions and allow the IOO to configure or limit interactions with external systems in accordance with organizational policy.

Parameter Value(s):

paragraph a. “require external systems to use approved security controls such as encrypted communications, authenticated access, activity logging, and compliance with applicable privacy and data-handling requirements.”

paragraph b. “personally owned, unmanaged, or unapproved devices and external storage media.”

Risk References and Resources:

ATT&CK for ICS Mitigations / Techniques: M0801 / T0868, T0886

NIST SP 800-82⁽⁴⁾: 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.

Standards: FIPS 140-3⁽¹⁸⁾, NIST SP 800-46⁽³⁰⁾

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

Responsible Party (M/I): M/I

Justification to Select: If external systems are authorized for use, the IOO must establish, document, and accept clear limits on their use, including the risks inherent in permitting access from systems outside the defined CCTV system boundary.

Guidance: The IOO should define and document specific limitations on the use of authorized external systems, including permitted functions, access scope, duration of access, and data handling restrictions. External systems may include vendor maintenance systems, contractor laptops, jump hosts, or other non-CCTV systems. Manufacturers and vendors are expected to provide capabilities that allow the IOO to enforce these limitations and prevent external systems from performing unauthorized actions or accessing functions beyond those explicitly approved.

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

Responsible Party (M/I): I

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

Guidance: The IOO develops policy and procedures that limit or prohibit the use of portable storage devices on CCTV devices, video management systems (VMS), storage systems, and associated management interfaces, except during authorized maintenance or operational activities performed by trained personnel.

If use is approved, the IOO ensures that:

- Devices are scanned for malware on a trusted system before connection to any CCTV component;

- Media are cryptographically protected (signed or write-protected) to prevent modification; and
- Transfers are logged and validated against approved configuration or operational baselines.

Manufacturers and vendors support this control by implementing CCTV software and firmware capabilities that can disable USB mass-storage functions, enforce read-only modes, or restrict file types and paths accessible from portable media.

Parameter Value(s):

“Restrict use to read-only, encrypted portable storage devices for authorized footage export; require documented chain-of-custody procedures and automatic media sanitization after transfer completion.”

Standards: FIPS 140-3⁽¹⁸⁾, NIST SP 800-56⁽³¹⁾, NIST SP 800-171⁽³⁹⁾, ISO/IEC 27002⁽²⁷⁾

AC-21, Information Sharing

Responsible Party (M/I): I

Justification to Select: Non-adversarial threat event "Mishandling of critical and/or sensitive information by authorized users" in table 4.

Guidance: The IOO should define and document policies governing the sharing of CCTV information with internal and external entities, including what information may be shared, with whom, and under what conditions. Information sharing policies should account for security sensitivity, privacy considerations, and operational need, and should ensure that only authorized information is disclosed to external parties such as vendors, contractors, or partner organizations.

Parameter Value(s):

paragraph a. "when sharing system logs, configuration data, or diagnostic reports containing security-relevant information with external entities such as vendors or service providers"

paragraph b. "automated access control decision tools, information labeling or tagging mechanisms, and/or user guidance procedures integrated into information-sharing workflows to prevent unauthorized disclosure."

Risk References and Resources:

ATT&CK for ICS Mitigations / Techniques:

- M0809 / T0882

ARC-IT Mechanisms:

- The organization should go through a process of classifying all sensitive data that it stores.
- Based on data classifications, an administrative process will determine sensitivity levels of various data types. Following this process, an authorization matrix will be generated and implemented to determine which type of data can be shared with which type of user.
- Organizations should maintain the principle of least privilege on sensitive data and only permit the minimum amount of data to be shared among users necessary to perform their normal job functions.

AC-24, Access Control Decisions

Responsible Party (M/I): M/I

Justification to Select: A CCTV system typically includes embedded firmware, one or more local or centralized management interfaces, and network connectivity to traffic management centers or other backend systems. These systems support multiple operational and maintenance functions, such as live video viewing, configuration, software updates, and diagnostics, often by different user roles and, in some cases, third-party vendors. Inadequate or inconsistently applied access controls can allow unauthorized viewing, manipulation, or modification of CCTV system functions. This control addresses the vulnerability of “Inadequate access controls applied” in table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: The IOO should define access authorization policies, roles, and control objectives for CCTV operational, administrative, and maintenance functions. Manufacturers and vendors are expected to provide mechanisms within the CCTV device, video management system (VMS), and associated management interfaces that evaluate access requests and enforce access control decisions prior to permitting access, in accordance with IOO-defined policy.

Parameter Value(s):

#1 “Implement mechanisms”

#2: Access control decisions are based on evaluation of:

- Authenticated user or system identity
- Assigned role or privilege level
- Requested CCTV function (e.g., live view, playback, export, configuration, firmware update, diagnostics)
- Applicable operational or maintenance conditions (e.g., approved maintenance window, remote vs local access)

AT Family – Awareness and Training

AT-3, Role-Based Training

Responsible Party (M/I): M/I

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

Guidance: The IOO establishes a structured, role-based training program that provides training at multiple layers, aligned to organizational responsibility and decision authority.

- **Executive and governance roles** (e.g., CISO, program leadership, privacy, and legal staff) receive training focused on cybersecurity risk management, regulatory and privacy obligations, threat trends affecting ITS, and oversight responsibilities.
- **Operational and technical roles** (e.g., system administrators, network and security engineers, integrators, and maintainers) receive detailed technical training addressing threats relevant to the CCTV and ITS environment, secure configuration and maintenance practices, monitoring and incident response procedures, and the security techniques used to mitigate identified risks.

- **Field and support personnel** receive training appropriate to their interaction with CCTV assets, including secure handling procedures, access restrictions, and reporting of anomalous or suspicious conditions.

Manufacturers and vendors ensure that development, integration, and support personnel receive role-appropriate training covering secure software development, configuration management, vulnerability remediation, and supply-chain security practices relevant to CCTV systems and connected infrastructure.

Parameter Value(s):

paragraph a. “Executive and governance personnel (e.g., CISO, program leadership, privacy or legal staff); CCTV manufacturers and integrators; system administrators; field technicians; and network and security engineers.”

paragraph a.1. “annually”

paragraph b. #1: “annually”

paragraph b. #2: “After identification of new threats, vulnerabilities, or adversary TTPs relevant to CCTV devices or the ITS environment.”

Risk References and Resources:

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

NIST SP 800-82⁽⁴⁾: 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: Threat event “Perform network sniffing of exposed networks” in table 3, Perform Reconnaissance and Gather Information.

The control applies to components that transmit or receive information, as communication paths outside the physical protection of a controlled boundary are exposed to the possibility of interception and modification.

Guidance: This control is primarily organizational, with the IOO responsible for identifying and documenting the events that must be logged to support security monitoring, incident response, and accountability. Manufacturers and vendors are expected to provide CCTV devices, video management systems (VMS), storage systems, and management interfaces with the capability to generate, retain, and export logs for the defined events. Logging capabilities should support both local and centralized collections consistent with the system architecture.

Parameter Value(s):

paragraph a. "system startup and shutdown, service and application startup and shutdown, application failures/exceptions, application configuration changes (e.g., application security profile), network connection and loss events (e.g., wireless or Ethernet connection), modifications to security-related settings, successful and unsuccessful logon attempts, software and firmware updates, creation/modification/deletion of accounts and account privileges (users and apps), accesses to files/directories used by software/firmware updates, unauthorized access attempts to corresponding private key operations (optional), network and firewall configuration changes, any changes to audit and audit reporting behavior, modifications to certificate trust lists, and unauthorized attempts to modify log files. Otherwise, the design details for logging are vendor specific (e.g., the event messages)."

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

paragraph e. "at least Quarterly"

Risk References and Resources:

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

NIST SP 800-53⁽²⁾: 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.

ARC-IT Mechanisms:

- The device provides a means to define a list of auditable activities. This should be based on the list of resources for which privileged access is required as discussed in Notes on Access Control.⁽¹³⁾
- The device provides a means to define and update a policy for auditing auditable activities.
- The device provides access control mechanisms to restrict read or write access to the list of auditable activities and to the audit policy.
- The device should support an audit policy in which a log is created that contains a list of all the distinct processes that have accessed or attempted to access each privileged function during one power-on time and may support additional audit policies.
- The device may provide a means for storing audit logs in an external location.

Standards: RFC 8446⁽¹⁴⁾; NTCIP 9014 v01.20, section B.2.⁽¹⁵⁾

AU-3, Content of Audit Records

Responsible Party (M/I): M/I

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

Guidance: This control is primarily technical in nature. The IOO defines the audit record content necessary to support security monitoring, incident response, forensic analysis, and accountability. Manufacturers and vendors are expected to ensure that CCTV devices, video management systems (VMS), storage systems, and associated management interfaces generate audit records containing sufficient detail to support these objectives.

At a minimum, audit records should capture information such as the date and time of the event, the type of event, the outcome (success or failure), the identity of the user, process, or system associated with the event, the role or privilege level involved (where applicable), the affected CCTV component or resource, and the origin of the request (e.g., local or remote access). Event message formats and internal logging implementations may be vendor-specific, provided the required information is recorded and accessible for review.

AU-4, Audit Log Storage Capacity

Responsible Party (M/I): M/I

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

Guidance: This control is both organizational and technical. The IOO defines audit log retention and availability requirements necessary to support security monitoring, incident response, and forensic analysis. Manufacturers and vendors are expected to ensure that CCTV devices, video management systems (VMS), storage systems, and associated management interfaces provide sufficient audit log storage capacity, or support reliable export to external log storage, to prevent loss or overwriting of audit records prior to review.

Parameter Value(s):

“Sufficient capacity to retain audit records for a minimum of 30 days of normal operations without overwriting, or until logs are successfully exported to an external log management system.”

Risk References and Resources:

ARC-IT Mechanisms: As specified in control.

ARC-IT Protocol Implementation Conformance Statement: Provides 4 megabytes of audit storage.

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

Responsible Party (M/I): M/I

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

Guidance: Where local audit log storage on CCTV devices is limited, it may be necessary to transfer audit records to alternate or centralized storage, such as systems located at the Traffic Management Center (TMC), where logs can be retained and reviewed. Depending on system architecture, audit logs may be transferred to centralized log management systems or storage platforms already used to support CCTV operations (e.g., VMS-integrated storage, NAS, or SAN). Manufacturers and vendors

are expected to provide reliable mechanisms to support secure and timely transfer of audit logs to prevent loss or overwriting of audit records.

Parameter Value(s):

“At a frequency sufficient to prevent audit records from being overwritten or lost, and at least weekly, or more frequently based on event volume and operational risk.”

Risk References and Resources:

NIST SP 800-82⁽⁴⁾: 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 are not maintained” in table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: This control is primarily technical in nature. The IOO defines which personnel or roles must be notified of audit processing failures and the organizational response expectations. Manufacturers and vendors are expected to provide capabilities within CCTV devices, video management systems (VMS), storage systems, and associated management interfaces to detect audit logging failures, generate notifications, and perform IOO-defined response actions when audit processing is disrupted.

Parameter Value(s):

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

paragraph a: #2 "1 hour"

paragraph b: "Generate alerts, attempt automated recovery of audit processing, and continue system operation while preventing loss or tampering of existing audit records."

Risk References and Resources:

ARC-IT Mechanisms:

- Device should support the identification of a device management service to which audit processing failures should be reported if connectivity is available.
- The ability to alter the device management service should be restricted to privileged users per AC-3.
- Device should identify information flows to the device management service as a secured information flow per AC-4 and should protect those information flows with an approved mechanism per SC-8.
- Device should report audit processing failure to the device management service if it has connectivity when the audit processing failure occurs.
- Device may maintain a backup logging service to be used to record failures in the audit processing service.
- Device should reboot its audit processing service and thereafter attempt to start processing again on a failure. If no successful audit processing occurs over three reboot attempts, the device should log a report via a different mechanism and suspend auditing.

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

Responsible Party (M/I): M/I

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

Guidance: This control is primarily technical in nature. The IOO defines alerting requirements for impending audit log storage exhaustion, including notification of recipients, timing, and threshold conditions. Manufacturers and vendors are expected to provide capabilities within CCTV devices, video management systems (VMS), storage systems, and associated management interfaces to monitor audit log storage utilization and generate warnings when IOO-defined thresholds are approached, allowing corrective action before audit records are lost or overwritten.

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 are not maintained” in table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: This control is primarily technical in nature and addresses the system's response to audit logging process failures. The IOO defines expectations for real-time or near-real-time notification and the required organizational response when audit logging failures occur. Manufacturers and vendors are expected to provide capabilities within CCTV devices, video management systems (VMS), storage systems, and associated management interfaces to detect audit logging process failures, generate immediate alerts, and support timely response actions to prevent loss of audit data or prolonged gaps in auditing.

Parameter Value(s):

- #1 See ARC-IT Mechanisms below.
- #2 See ARC-IT Mechanisms below.
- #3 “Minimally but not limited to: auditing software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.”

Risk References and Resources:

NIST SP 800-82⁽⁴⁾: Organizational requirements may require storage of exceptionally large amounts of data, which ITS components may not be able to support directly.

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

Responsible Party (M/I): I

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

Guidance: The IOO establishes policies and procedures for the routine review, analysis, and reporting of audit records generated by CCTV devices, video management systems (VMS), storage systems, and associated management interfaces. Audit review should focus on identifying anomalous, unauthorized, or unexpected activity, including failed or suspicious access attempts, configuration changes, system or application failures, and indicators of misuse or compromise. Particular attention should be given to audit records associated with remote access, privileged actions, and access to stored video content to ensure potential security or privacy issues are identified and addressed in a timely manner.

Parameter Value(s):

paragraph a.1 "At least quarterly"

paragraph a.2. "Minimally but not limited to failed and successful access attempts, use of privileged accounts or functions, system and application failures, configuration changes, and other security-relevant events."

paragraph b. "Administrators"

Risk References and Resources:

ATT&CK for ICS Mitigations / Techniques:

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

NIST SP 800-82⁽⁴⁾: Example compensating controls include manual mechanisms or procedures. For devices where audit records cannot be feasibly collected, periodic manual review may be necessary.

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

Responsible Party (M/I): I

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

Guidance: The IOO should define which systems and services are included in centralized audit record review and analysis, as well as the policies and procedures governing how audit data is aggregated, correlated, and reviewed. Centralized review should encompass audit records from CCTV devices, video management systems (VMS), storage systems, and associated management interfaces to support consistent monitoring, trend analysis, and detection of anomalous or unauthorized activity. Where applicable, audit records associated with remote access, remote storage, remote clients, or legacy components (e.g., DVRs supporting analog cameras) should be included to ensure comprehensive visibility across the CCTV environment.

AU-6(5), Audit Record Review, Analysis, and Reporting | Integrated Analysis of Audit Records

Responsible Party (M/I): I

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

Guidance: The IOO establishes policies and procedures to integrate audit records from CCTV devices, video management systems (VMS), storage systems, and associated management interfaces with other relevant security and operational data sources. Integrated analysis may include correlation with vulnerability scanning results, system and network monitoring data, configuration and performance metrics, or other security-relevant information to improve detection, context, and prioritization of anomalous or unauthorized activity. The scope of integrated analysis should include audit records associated with remote access, remote storage, and other networked components supporting CCTV operations.

Parameter Value(s):

#1 "vulnerability scanning information, system monitoring information, and performance data"

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

Responsible Party (M/I): I

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

Guidance: The IOO establishes policies and procedures to correlate audit records from CCTV devices, video management systems (VMS), storage systems, and management interfaces with information from physical monitoring and access controls. Physical monitoring information may include logs or alerts associated with access to camera housings, mounting enclosures, field cabinets, control room equipment, local network switches, or other supporting infrastructure. Correlating cyber audit records with physical access or tamper events supports detection of unauthorized access, equipment compromise, or misuse that may not be evident from cyber logs alone.

AU-7, Audit Record Reduction and Report Generation

Responsible Party (M/I): I

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

Guidance: The IOO establishes policies and procedures for reducing large volumes of audit records into summarized, filtered, or aggregated information and for generating audit reports that support security monitoring, incident detection, and management oversight. Audit record reduction may include filtering routine or expected activity, highlighting anomalous or policy-relevant events, and organizing audit data by system, user role, or event type. The IOO also defines when audit reports are generated, the content and level of detail required, and the personnel or roles to whom reports are provided when suspicious activity, policy violations, or other security-relevant conditions are identified.

Risk References and Resources:

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

AU-9, Protection of Audit Information

Responsible Party (M/I): M/I

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

Guidance: This control is primarily technical in nature. The IOO defines which roles are authorized to access audit information and the organizational expectations for notification or response when audit information is accessed or altered. Manufacturers and vendors are expected to provide mechanisms within CCTV devices, video management systems (VMS), storage systems, and associated management interfaces to protect audit records from unauthorized access, modification, and deletion, including enforcing access controls, preserving audit record integrity, and preventing or detecting tampering.

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 of AC-3.

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

Responsible Party (M/I): M

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

Guidance: This control is technical in nature and addresses protection of audit information through architectural separation. Manufacturers and vendors are expected to provide capabilities that allow audit records generated by CCTV devices, video management systems (VMS), and associated components to be stored on separate physical systems or components from those being audited. Such separation reduces the risk that an attacker or malicious insider can modify or delete audit records to conceal unauthorized activity. Separate storage may include centralized log servers, VMS-integrated repositories, or dedicated storage systems supporting CCTV operations.

Parameter Value(s):

“At least weekly, or more frequently based on audit volume and operational risk.”

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 are not maintained” in table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: This control is technical in nature and addresses protection of audit record integrity. Manufacturers and vendors are expected to implement cryptographic mechanisms that provide integrity protection and tamper detection for audit records stored by CCTV devices, video management systems (VMS), and associated components. Such mechanisms may include cryptographic hashes, digital signatures, or message authentication codes that allow unauthorized modification or deletion of audit records to be detected during review or forensic analysis.

Risk References and Resources:

ARC-IT Mechanisms: See control AU-09.

Standards: FIPS 197⁽²⁴⁾

AU-11, Audit Record Retention

Responsible Party (M/I): M/I

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

Guidance: Manufacturers and vendors are expected to ensure that CCTV devices, video management systems (VMS), storage systems, and associated management interfaces securely retain audit records for the IOO-defined retention period, including in disconnected or intermittently connected environments. Audit records must remain available for operational review, incident response, forensic analysis, and legal or regulatory inquiries. Retention mechanisms should preserve audit record integrity and availability for the full retention period and prevent premature deletion or loss of records.

Parameter Value(s):

"3 Years"

Standards: FIPS 197⁽²⁴⁾

AU-12, Audit Record Generation

Responsible Party (M/I): M

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

Guidance: This control is technical in nature. Manufacturers and vendors are expected to implement audit record generation capabilities within CCTV devices, video management systems (VMS), storage systems, and associated management interfaces. Audit record generation must support the events, content, and scope defined by the organization through the application of controls AU-2 (Event Logging) and AU-3 (Content of Audit Records), ensuring that security-relevant activities are consistently and reliably captured at the source.

Parameter Value(s):

paragraph a. "CCTV devices, video management systems (VMS), storage systems, and associated management or network components within the CCTV system boundary."

paragraph b. "Audit administrator or equivalent privileged role responsible for audit configuration and oversight."

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 are not maintained" in table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: This control is technical in nature. Manufacturers and vendors are expected to implement mechanisms that restrict changes to audit record generation to explicitly authorized roles and ensure that all such changes are themselves audited. The audit record generation capability must support configurable event selection criteria and timing thresholds so that authorized individuals can adjust audit settings in accordance with organizational policy, while maintaining accountability and traceability for all changes.

Parameter Value(s):

#1 "Local device administrator, Audit administrator"

#2 "CCTV 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⁽⁴⁾: Example compensating controls include employing non-automated mechanisms or procedures.

AU-13, Monitoring for Information Disclosure

Responsible Party (M/I): I

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

Guidance: The IOO establishes policies and procedures to monitor indicators of unauthorized disclosure of CCTV-related information. Monitoring activities may include review of audit records, network traffic analysis, alerts from external threat intelligence sources, vulnerability disclosure notifications, and other security-relevant information. Particular attention should be given to external connections and interfaces supporting CCTV operations, such as connections to back-office systems,

maintenance devices, remote access services, or third-party support systems, to detect potential exposure of video content, system configurations, credentials, or other sensitive information.

Parameter Value(s):

paragraph a.#1 "cyber threat intelligence feeds and vulnerability disclosure sites such as Common Vulnerabilities and Exposures (CVE) listings"

paragraph a.#2 "Weekly as part of regular cybersecurity situational awareness and immediately upon notification of a suspected breach or vendor vulnerability disclosure"

paragraph b.#1 "System Administrator, Security Administrator, Incident Response personnel, and any other pertinent security personnel"

paragraph b.#2 "initiate the incident response process and assess potential impact to CCTV operations or data; notify affected external entities"

AU-14, Session Audit

Responsible Party (M/I): M/I

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

Guidance: This control is primarily technical in nature. Manufacturers and vendors are expected to provide mechanisms to audit and record user activity within authenticated sessions on CCTV devices, video management systems (VMS), storage systems, and associated management interfaces. Session audit records may include session start and end times, user identity, accessed interfaces, commands issued, configuration changes, and other security-relevant actions performed during the session. The IOO defines which roles are authorized to review session audit information and how session audit data is used to support accountability, monitoring, and incident investigation.

Parameter Value(s):

paragraph a.#1 "Security Administrators or equivalent roles responsible for audit review and investigation."

AU-16, Cross-Organizational Audit Logging

Responsible Party (M/I): M/I

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

Guidance: The IOO establishes policies and agreements governing the exchange and correlation of audit records when CCTV information crosses organizational boundaries, such as between infrastructure owners, traffic management centers (TMCs), service providers, or law enforcement entities. Cross-organizational audit logging should ensure that security-relevant events such as access requests, authentication outcomes, and authorization decisions can be traced to authenticated user or system identities at the originating organization. Manufacturers and vendors are expected to provide capabilities within CCTV devices, video management systems (VMS), and associated management interfaces to generate and export audit records in a manner that preserves identity, context, and integrity across organizational boundaries. These mechanisms should support

secure exchange and be documented through formal information exchange or interconnection agreements.

Parameter Value(s):

#1 secure, encrypted data exchange

#2 "security-relevant audit records, including access events, authentication and authorization decisions, and network or communication audit data associated with CCTV operations."

Standards: NIST SP 800-52⁽³⁷⁾, ISO/IEC 18033-3⁽³⁸⁾

CA Family – Assessment, Authorization, and Monitoring

CA-3, Information Exchange

Responsible Party (M/I): I

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

Guidance: The IOO establishes and enforces an approval process for all systems and services that exchange information with the CCTV system. This includes connections to video management systems (VMS), video recording, and processing systems (e.g., NVRs, DVRs), centralized storage platforms, analytics services, and external organizational systems. For each approved interconnection, the IOO documents the purpose of the exchange, the types of information shared, security and privacy requirements, and applicable operational constraints. Approved interconnections must align with established cybersecurity, privacy, and operational requirements and be formally authorized prior to use.

Parameter Value(s):

paragraph a. "interconnection security agreements and information exchange security agreements"

paragraph c. "semi-annually"

Risk References and Resources:

ATT&CK for ICS Mitigations / Techniques:

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

NIST SP 800-82⁽⁴⁾: Organizations perform risk-benefit analysis to determine whether an ITS should be connected to other systems. The authorizing official fully understands the organizational information security policies and procedures; the ITS security policies and procedures; the risks to organizational operations and assets, individuals, other organizations, and the Nation Select associated with the connection to other systems; the individuals and organizations that operate and maintain the systems, including maintenance contractors or service providers; and the specific health, safety, and environmental risks associated with a particular interconnection. Connections from the ITS environment to other security zones may cross the authorization boundary such that two different authorizing officials may be required to approve the connection. Decisions to accept risk are documented.

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

Responsible Party (M/I): I

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

Guidance: The IOO establishes and documents transfer authorization requirements for information exchanged with the CCTV system. This includes pre-authorizing the individuals, systems, and organizational entities permitted to send, receive, or retrieve CCTV-related information, as well as defining the types of information authorized for transfer and the conditions under which transfers are permitted. Transfer authorizations are documented through interconnection security agreements or information exchange agreements and ensure that only approved, trusted entities can exchange information with the CCTV system in accordance with security, privacy, and operational policies.

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

Responsible Party (M/I): I

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

Guidance: The IOO establishes and documents policies and procedures for identifying, assessing, and approving downstream information exchanges associated with the CCTV system. This includes understanding where CCTV information may be further shared, processed, or stored beyond the initially authorized system-to-system exchange. Examples include video management systems (VMS), remote monitoring or mobile access applications, analytics platforms, backup or archival systems, and external organizational services. The IOO ensures that downstream information exchanges are evaluated for security and privacy risk and are explicitly authorized as part of the information exchange approval process. Where the security posture or use of downstream systems cannot be adequately validated, information exchanges involving those paths are restricted or terminated to protect the confidentiality, integrity, and availability of CCTV information.

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: This is an organizational control implemented by the IOO. The IOO establishes and maintains a plan of action and milestones (POA&M) to document, track, and manage the remediation of identified security control weaknesses associated with the CCTV system. During design, development, or integration, the IOO may require the manufacturer or vendor to identify known control gaps or limitations and provide corresponding remediation plans as part of system delivery. The IOO uses the POA&M to understand which security controls have not been fully or satisfactorily implemented, assess the associated operational and cybersecurity risk, and determine whether the CCTV system may be approved for deployment and operation within the ITS environment. Where unacceptable risks are identified, the IOO may require remediation, implement compensating controls, or delay deployment until risk is reduced to an acceptable level.

Parameter Value(s):

“at least quarterly or as weaknesses (e.g., non-compliant controls) are corrected”

Risk References and Resources:

NIST SP 800-82⁽⁴⁾: Corrective actions identified in assessments may not be immediately actionable in an ITS environment; therefore, short-term mitigations may be implemented to reduce risk as part of the gap closure plan or plan of action and milestones.

CA-6, Authorization

Responsible Party (M/I): I

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

Guidance: This is an organizational control implemented by the IOO. The IOO authorizes the operation of the CCTV system by explicitly accepting the cybersecurity and operational risks associated with its deployment and use. While the IOO is not required to implement the full set of roles, artifacts, and processes defined in NIST SP 800-37, there must be a designated senior official who is informed of the identified risks and formally authorizes the system to operate within the ITS environment.

This authorization decision is informed by available risk information, including security control implementation status, identified weaknesses, and compensating controls. As ITS organizations mature in their cybersecurity practices, authorization activities may evolve toward a more formal, enterprise-level risk management approach consistent with NIST SP 800-39, which addresses risk framing, assessment, response, and ongoing monitoring.

Parameter Value(s):

paragraph e. “At least annually, or upon significant system, threat, or operational 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: This control is primarily organizational in nature and establishes the continuous monitoring strategy for the CCTV system with an emphasis on maintaining ongoing visibility into security posture. The IOO determines the scope, depth, and frequency of monitoring activities based on system criticality, connectivity, and risk, prioritizing the detection of unauthorized access, misuse of privileges, unexpected information flows, configuration or integrity changes, and other security-relevant conditions.

Continuous monitoring may include both automated and manual activities and can leverage telemetry, logs, and alerts provided by CCTV devices, video management systems (VMS), storage platforms, and supporting network infrastructure. Operational and availability indicators (e.g., video stream loss, bandwidth anomalies, or storage exhaustion) may be monitored as supporting signals when correlated with potential security events. Monitoring activities are designed to provide timely awareness without adversely affecting CCTV operations

Parameter Value(s):

paragraph a. "security-relevant events and conditions including, but not limited to: unauthorized or failed access attempts; remote access outside approved timeframes; unauthorized PTZ commands or camera configuration changes; unexpected or unapproved information flows or video stream access; camera tamper detection events; firmware or configuration integrity alerts; and availability indicators (e.g., video stream loss, bandwidth anomalies, or storage exhaustion) when correlated with potential security events."

paragraph b. #1 "real time or daily"

paragraph b. #2 "weekly"

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

paragraph g. #2 "daily"

Risk References and Resources:

ATT&CK for ICS Mitigations / Techniques:

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

NIST SP 800-82⁽⁴⁾: 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 systems 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.

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 automated monitoring capabilities required to support continuous visibility into the security posture of the CCTV system, including the accuracy, timeliness, and availability of monitoring results. Automation is used to supplement manual monitoring and enable scalable detection of security-relevant conditions such as unauthorized access, anomalous information flows, configuration drift, and integrity changes.

Manufacturers and vendors implement capabilities within the CCTV device, associated management systems, and supporting infrastructure that enable automated collection, correlation, and reporting of

monitoring data. Automation may be implemented at the device level, upstream network components, or centralized monitoring platforms (e.g., TMC systems), as appropriate for the system architecture and operational constraints.

Parameter Value(s):

“Automated mechanisms such as log collection and analysis tools, configuration compliance or drift detection scanners, vulnerability scanning tools appropriate for the ITS environment, and alerting or visualization dashboards integrated into the continuous monitoring process.”

CA-8, Penetration Testing

Responsible Party (M/I): I

Justification to Select: Vulnerability “Lack of a vulnerability management program” in table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions. Penetration tests serve to examine whether an IOO's security policies are genuinely effective, while also identifying vulnerabilities in a system and providing awareness of/enhancing cybersecurity hygiene.

Guidance: This is an organizational control implemented by the IOO. The IOO determines whether, when, and how penetration testing is conducted for the CCTV system, taking into account operational risk, system criticality, and safety considerations. Penetration testing is used to evaluate the effectiveness of implemented security controls and to identify exploitable weaknesses that could affect the confidentiality, integrity, or availability of CCTV devices, video management systems, and associated infrastructure.

Penetration testing activities are carefully scoped, authorized, and coordinated to avoid adverse impacts on traffic operations or roadway safety. Where direct testing of production of ITS components presents unacceptable risk, the IOO may employ alternative approaches such as testing in replicated, segmented, or simulated environments. Results of penetration testing are documented and used to inform corrective actions, compensating controls, or risk acceptance decisions.

Parameter Value(s):

#1 "at least annually"

#2 “high-impact components, including CCTV devices, video management systems, storage platforms, and supporting IP-based network interfaces and services within the authorized testing scope.”

Risk References and Resources:

NIST SP 800-82⁽⁴⁾: 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 of 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.

CA-9, Internal System Connections

Responsible Party (M/I): M/I

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

Guidance: The IOO establishes and documents policies and procedures for authorizing and managing internal system connections within the CCTV architecture. This includes identifying and approving connections among cameras, video management systems (VMS), recording and processing components, and storage systems based on defined security, privacy, and operational requirements. Internal connections are documented to provide visibility into trusted relationships and data flows within the system boundary. The IOO reviews internal connections periodically and updates authorizations when system components are added, removed, or reconfigured, or when risk conditions change.

Parameter Value(s):

paragraph a. “IP cameras, multiplexers, internal switching components, direct-attached storage devices, video recorders, and video management systems.”

paragraph c. “Decommissioning of a device, network or architecture reconfiguration, detected security incidents, or when an internal connection is no longer operationally required.”

paragraph d. “At least annually”

Risk References and Resources:

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

CA-9(1), Internal System Connections | Compliance Checks

Responsible Party (M/I): I

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

Guidance: Prior to authorizing internal system connections within the CCTV architecture, the IOO performs compliance checks to verify that each connected component meets applicable security, privacy, and operational requirements. For each proposed connection, the IOO documents relevant interface characteristics, including communication protocols, encryption or protection mechanisms, and the types of videos, metadata, or control information exchanged. Compliance checks confirm alignment with approved baseline configurations and organizational policies before the connection is established or reauthorized. Results of compliance checks are used to inform connection approval, restriction, or denial decisions.

CM Family – Configuration Management

CM-2, Baseline Configuration

Responsible Party (M/I): I

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

Guidance:

The IOO develops documents and maintains a baseline configuration for the CCTV system and its supporting components. The baseline configuration defines approved settings for CCTV devices, video management systems (VMS), storage platforms, and supporting network interfaces, including security-relevant parameters such as authentication methods, access control roles, logging settings, encryption configurations, remote access settings, and approved services or ports.

Baseline configurations are placed under configuration control and are reviewed and updated at defined intervals, following security incidents, or when system components, software, or operational requirements change. The baseline serves as the reference point for system deployment, configuration validation, change management, and compliance checks across the CCTV lifecycle.

CM-3, Configuration Change Control

Responsible Party (M/I): M/I

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

Guidance The IOO establishes and enforces configuration change control procedures for the CCTV system to ensure that all changes to approved baseline configurations are reviewed, authorized, documented, and tracked. Configuration change control applies to CCTV devices, video management systems (VMS), storage components, firmware, software, and supporting network interfaces, and include but are not limited to access controls, authentication mechanisms, logging parameters, network connectivity, and secure features.

Changes to configuration settings are evaluated for security and operational impact prior to implementation. The IOO periodically reviews configuration changes to verify continued compliance with approved baselines. Manufacturers and vendors support this control by providing mechanisms to record, log, and report configuration changes in a manner that supports review, auditing, and troubleshooting.

Parameter Value(s):

paragraph b.1. "semi-annual

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

Risk References and Resources:

NIST SP 800-82⁽⁴⁾: Configuration of 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 are not under configuration management” in Table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: The IOO conducts and documents impact analyses prior to implementing changes to the CCTV system to evaluate potential effects on cybersecurity, privacy, operational performance, and roadway safety. Impact analyses consider how proposed changes (for example configuration updates, firmware or software changes, network modifications, or integration with new systems) may affect existing security controls, information flows, system availability, and operational use cases.

Results of impact analyses are used to inform change approval decisions, identify required mitigations or compensating controls, and ensure that changes do not introduce unintended vulnerabilities or degrade CCTV system functionality within the ITS environment.

Risk References and Resources:

NIST SP 800-82⁽⁴⁾: 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 are not under configuration management” in Table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: The IOO establishes and enforces physical and logical access restrictions for initiating and executing changes to the CCTV system. These restrictions apply to modifications of hardware, firmware, software, configuration settings, and operational procedures that affect system behavior or security posture. Only authorized and qualified personnel are permitted to perform configuration or maintenance changes, and their access is limited to the functions and components required for their assigned roles.

Access restrictions are implemented to clearly separate operational use of the CCTV system (e.g., viewing video or monitoring traffic conditions) from configuration and maintenance activities. Where supported by technology, the IOO employs mechanisms such as role-based access controls, maintenance modes or physical locks to prevent unauthorized or accidental changes to system configuration.

Risk References and Resources:

NIST SP 800-82⁽⁴⁾: Some ITS devices allow for the configuration and use of mode to 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 are not under configuration management” in Table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance:

The IOO implements dual authorization for selected configuration and security-relevant changes to the CCTV system where the risk of unauthorized, erroneous, or malicious modification is significant. Dual authorization requires independent approval by a second authorized individual before changes are executed, ensuring that no single person can unilaterally modify critical system settings.

This enhancement is applied to changes that affect system security posture, access control, data protection, or operational integrity, and may be implemented through administrative procedures, workflow approvals, or technical mechanisms that enforce separation of duties. Dual authorization requirements are defined in policy and tailored to balance security assurance with operational practicality in the ITS environment.

Parameter Value(s):

“Camera firmware updates, access control rule changes, credential creation or modification, and storage retention policy changes”

CM-6, Configuration Settings

Responsible Party (M/I): M/I

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

Guidance: This control is both organizational and technical in nature. The IOO defines and documents required configuration settings for the CCTV system based on operational, security, privacy, and interoperability requirements. Configuration settings include security-relevant parameters such as authentication and authorization behavior, logging and audit settings, encryption options, network services and ports, remote access features, and operational camera behaviors.

Manufacturers and vendors support this control by implementing CCTV devices, video management systems (VMS), and supporting components that allow required configuration settings to be applied, validated, and maintained throughout the system lifecycle. Where manufacturer-recommended configuration baselines are provided, the IOO reviews and tailors those settings to align with organizational policy and ITS operational needs. Configuration settings are maintained under configuration control and are updated as operational requirements, standards, or risk conditions change.

Parameter Value(s):

paragraph a. National Transportation Communications for ITS Protocol Connected Transportation Interoperability (NTCIP) 1205

paragraph c. #1 “IP cameras, multiplexers, internal switching components, direct-attached storage devices, video recorders, and video management systems.”

paragraph c. #2 “operational requirements from NTCIP 1205”

CM-7, Least Functionality

Responsible Party (M/I): M/I

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

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

Guidance: This control is primarily technical and is implemented by the manufacturer/vendor through system design and default configuration. The IOO defines and documents the mission-essential functions required for CCTV operation and specifies which functions, ports, protocols, services, and interfaces must be disabled, restricted, or conditionally enabled.

CCTV devices, VMS components, and supporting infrastructure are configured to expose only those capabilities necessary for traffic surveillance and system management. Non-essential services, development or debug interfaces, and unused network protocols are disabled by default and may only be enabled through authorized administrative action.

To support consistent risk management across ITS deployments, the IOO may maintain an allowlist of approved functions, ports, protocols, and services applicable to CCTV systems. Technical mechanisms such as host-based firewalls, service whitelisting, secure boot, and runtime monitoring are used to enforce least functionality and detect unauthorized or unexpected services.

Parameter Value(s):

paragraph a. "video capture, encoding, and secure transmission to the Video Management System (VMS); pan-tilt-zoom (PTZ) control; camera status and health monitoring; event and alarm signaling (e.g., motion detection, tamper alarm, loss-of-signal); and authenticated administrative access for configuration, diagnostics, and firmware verification"

paragraph b. "disabled or restricted by default: SSH except during explicitly authorized maintenance or firmware update activities; JTAG and UART debug interfaces; unused network ports; legacy or insecure protocols; and non-essential operating system services."

Risk References and Resources:

NIST SP 800-82⁽⁴⁾: The organization implements the 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.

ARC-IT Mechanisms:

- Device should expose only those services required to operate (FTP, secure shell [SSH], telnet, web interface, etc.).

- Device should enable disabling all system services and applications that are not essential to operation.
- Devices should support data loss prevention policies.
- The device should implement one or both of the following:
 - The device requires that all software installed is signed (corresponding to ongoing privileged access in the language of Notes on Access Control(13)).
 - If this approach is taken, the integrity of the verification key should be protected by local hardware, either by directly storing the key in local hardware, or by creating a chain of trust from the key to a hardware-protected key. The hardware protection should be equivalent to Federal Information Processing Standard (FIPS) 140-2⁽¹⁶⁾ level 2, 3, or 4 as specified in Notes on Access Control.⁽¹³⁾
 - The device allows unsigned software to be installed only by an authenticated user with periodic privileged access to the specific resources necessary for program installation, i.e., it does not automatically boot into a state where that access is permitted.
 - If this approach is taken, the device should require that the authenticated user is authenticated using two-factor authentication and that at least one of the two factors is protected by cryptographic hardware on the device. See IA-2 for further description.

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: This control is primarily technical and is implemented by the manufacturer/vendor through platform design and execution controls. CCTV devices and associated software components are configured to prevent the execution of unauthorized programs, scripts, or binaries, including those introduced through removable media, remote management interfaces, update mechanisms, or embedded auto-execution features.

The IOO defines policies governing allowable software execution, including prohibitions on auto-execution, side-loading of applications, and execution of unsigned or unverified code. The manufacturer/vendor supports these policies by implementing execution controls such as application allowlisting, signed-code enforcement, disabling auto-run features, and restrictions on interpreters or shell access.

This control is particularly important for field-deployed CCTV devices that may be physically accessible or intermittently connected, where unauthorized code execution could compromise surveillance integrity or enable persistent access.

Parameter Value(s):

“Only manufacturer-signed and organization-approved firmware, applications, and scripts may execute on CCTV devices; automatic execution of code from removable media, network shares, or external interfaces is prohibited; interpreters, shells, and debug execution environments are disabled or restricted to authorized maintenance modes.”

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

Responsible Party (M/I): M/I

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

Guidance: The IOO establishes a deny-by-exception policy for software execution on CCTV systems, whereby only explicitly authorized and approved software is permitted to execute. Any software, scripts, services, or code modules not explicitly approved are prohibited from execution.

Manufacturers and vendors support this control by implementing technical mechanisms that enforce execution allowlisting, such as signed-code verification, application allowlists, secure boot enforcement, or runtime execution controls. These mechanisms ensure that unauthorized software cannot execute, even if present on the system, and that execution controls remain effective in disconnected or field-deployed environments.

Parameter Value(s):

paragraph c. “review and update the list of authorized software at least annually, or upon firmware updates, software version changes, or introduction of new CCTV system components.”

CM-7(5), Least Functionality | Least Functionality | Authorized Software – Allow 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: This control is both organizational and technical. The IOO identifies and approves the specific software components authorized to execute the CCTV system and adopts a deny-all, permit-by-exception execution model. Only software explicitly authorized by the IOO is permitted to run; all other software execution is prohibited by default.

Manufacturers and vendors support this control by designing CCTV devices, firmware, operating systems, and associated management components to enforce application allowlisting through mechanisms such as signed-code verification, secure boot, and runtime execution controls. The authorized software set is expected to be relatively static for CCTV systems, making allowlisting practical and effective.

The IOO reviews and updates the authorized software list as needed throughout the system lifecycle and ensures that changes are reflected in configuration settings. If the authorized software set cannot be maintained as relatively static, CM-7(4) should be implemented instead.

Parameter Value(s):

paragraph a. “operating system kernels; signed firmware images; management and configuration applications; credential and key management components; video codec libraries; and network communication services required for CCTV operation.”

paragraph c. “at least annually”

Risk References and Resources:

NIST SP 800-82⁽⁴⁾: The set of applications that run in ITS is relatively static, making allowlisting practical. The U.S. Department of Homeland Security recommends using application allowlisting for ITS equipment.

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 are not under configuration management” in Table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: This control is both organizational and technical. The IOO defines and maintains a list of authorized hardware components permitted for use within the CCTV system and identifies hardware that is explicitly prohibited from connection or deployment. Authorized hardware includes cameras, storage devices, networking components, and peripherals required to support CCTV operations.

Manufacturers and vendors support this control by designing CCTV devices, VMS components, and supporting infrastructure to prevent or restrict the use of unauthorized hardware through technical mechanisms such as interface disabling, device authentication, hardware allowlisting, or configuration enforcement. Unauthorized hardware connections—whether introduced through maintenance activities, component replacement, or peripheral attachment—are prevented, detected, or generate alerts.

The IOO reviews and updates authorized hardware lists throughout the system lifecycle to reflect approved product changes, supply chain updates, or security requirements, and ensures configuration enforcement remains aligned with approved hardware inventories.

Parameter Value(s):

paragraph a. “agency-approved and/or Open Network Video Interface Forum (ONVIF)-compliant cameras, lenses, housings, mounts, monitors, switchers or multiplexers, and video recorders listed on the state DOT qualified products list, with FIPS 140-3–validated cryptographic modules for recorders and storage devices where encryption is required.”

paragraph c. “at least annually”

CM-8, System Component Inventory

Responsible Party (M/I): I

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

Guidance:

The IOO develops documents and maintains an accurate inventory of all system components that comprise the CCTV architecture. The inventory includes hardware, software, firmware, and logical components sufficient to support configuration management, vulnerability management, incident response, and least functionality enforcement.

For CCTV systems, the inventory typically includes cameras, lenses and housings (where applicable), video processing systems (e.g., DVRs, NVRs, multiplexers), video management systems (VMS), storage servers, network switches, and supporting operating systems, firmware, and applications. Inventory information is maintained throughout the system lifecycle and updated when components are added, replaced, upgraded, or decommissioned.

The system component inventory supports enforcement of controls such as CM-7 (Least Functionality), CM-6 (Configuration Settings), CM-5 (Access Restrictions for Change), and vulnerability and patch management activities.

Parameter Value(s):

Paragraph 5. “Unique identifier, manufacturer and model (where applicable), firmware and software version, and date of last configuration update or firmware change.”

Paragraph b. “semi-annual”

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

Responsible Party (M/I): I

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

Guidance:

The IOO updates the system component inventory whenever CCTV components are installed, replaced, relocated, or removed. Inventory updates occur as part of standard installation, maintenance, repair, and decommissioning activities, including field replacement of cameras, storage devices, network components, or supporting software and firmware.

Inventory updates are performed in a timely manner to ensure that the inventory accurately reflects the deployed CCTV architecture and supports configuration management, vulnerability tracking, and incident response activities.

CM-9, Configuration Management Plan

Responsible Party (M/I): I

Justification to Select: Vulnerability “Poor configurations are used” in Table 5, Section Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance:

The IOO develops, documents, and implements a configuration management plan for the CCTV system that governs how hardware, firmware, software, and configuration settings are established, maintained, and changed throughout the system lifecycle. The plan defines roles and responsibilities (e.g., system administrators, security administrators, field technicians), configuration baselines, change control procedures, approval authorities, documentation requirements, and mechanisms for tracking and auditing configuration changes.

The configuration management plan addresses both centrally managed components (e.g., VMS, storage systems, network infrastructure) and field-deployed CCTV devices, accounting for installation, maintenance, replacement, and decommissioning activities. The plan ensures that configuration management practices support secure, reliable, and continuous traffic surveillance operations without adversely impacting availability or roadway safety.

The configuration management plan aligns with and supports related controls in the CM family, including baseline configuration, change control, least functionality, authorized software and hardware, and system component inventory.

Parameter Value(s):

paragraph d. "System Administrator and/or Security Administrator responsible for configuration management plan development, maintenance, and enforcement."

CM-11, User-installed Software

Responsible Party (M/I): M/I

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

Guidance:

This control is primarily organizational and is implemented through policy, with technical enforcement provided by the manufacturer/vendor. The IOO establishes policies governing whether and under what circumstances software installation by users is permitted on CCTV systems. In typical ITS CCTV deployments, user-installed software is prohibited by default and permitted only as a documented exception for authorized maintenance or recovery activities.

Where software installation is permitted, the IOO restricts this capability to specifically authorized privileged roles and defines conditions under which installation may occur (e.g., approved maintenance windows, dual authorization, verified software sources). The manufacturer/vendor supports this control by implementing technical mechanisms that prevent unauthorized installation, enforce signature verification, restrict installation interfaces, and ensure that all installation activities are logged and auditable.

The IOO monitors compliance with user-installed software policies and investigates deviations to ensure continued alignment with configuration baselines and least functionality objectives.

Parameter Value(s):

paragraph a. "system lockdown to prevent local software execution; mandatory cryptographic signature verification; and centralized, approved software deployment from the TMC using dual authorization."

paragraph b. "role-based access control restricting software installation privileges"

paragraph c. "continuously through automated logging with monthly review"

Risk References and Resources:

ARC-IT Mechanisms: As specified in CM-7.

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 are not under configuration management" in Table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: This is primarily a technical control, and it applies to privileged operational users, as they are the only users who can install software. However, the IOO conveys to the manufacturer/vendor

the requirement for the CCTV to be designed and built to allow installation of software only with explicit privileged status. Note the linkage to related controls AC-5, and The IOO defines, documents, and maintains an authoritative description of where CCTV information is processed, transmitted, and stored throughout the system architecture. This includes identifying the system components and environments in which video data, snapshots, metadata, logs, and configuration files reside, such as cameras, roadside cabinets, video management systems (VMS), storage servers, backup repositories, and any cloud or offsite storage locations.

The information location documentation accounts for both steady-state operation and transient conditions, including buffering on cameras, temporary storage during transmission, and replication or backup processes. This control supports protection against unauthorized disclosure by ensuring the IOO understands where sensitive surveillance data exists, how it flows between components, and which environments require additional safeguards.

Information location details are kept current and are used to inform access control decisions, encryption requirements, information flow enforcement, incident response, and data retention policies.

CM-12, Information Location

Responsible Party (M/I): I

Justification to Select: Threat "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, documents, and maintains an authoritative description of where CCTV information is processed, transmitted, and stored throughout the system architecture. This includes identifying the system components and environments in which video data, snapshots, metadata, logs, and configuration files reside, such as cameras, roadside cabinets, video management systems (VMS), storage servers, backup repositories, and any cloud or offsite storage locations.

The information location documentation accounts for both steady-state operation and transient conditions, including buffering on cameras, temporary storage during transmission, and replication or backup processes. This control supports protection against unauthorized disclosure by ensuring the IOO understands where sensitive surveillance data exists, how it flows between components, and which environments require additional safeguards.

Information location details are kept current and are used to inform access control decisions, encryption requirements, information flow enforcement, incident response, and data retention policies.

Risk References and Resources:

NIST SP 800-82⁽⁴⁾: Organizations identify specific information types or components to track where information is being processed and stored. Information to consider in the ITS environment may include shared account passwords, PLC backup files, detailed network drawings, and risk assessments that identify specific threats to the environment.

CM-13, Data Action Mapping

Responsible Party (M/I): I

Justification to Select: Threat "Obtain sensitive information through network sniffing of external networks" in table 3, Achieve Results (i.e., cause adverse impacts, obtain information).

Guidance:

The IOO develops and maintains a data action map that documents how CCTV data is created, processed, transmitted, stored, accessed, and disposed of across the system lifecycle. The data action map identifies key data actions (e.g., video capture, buffering, transmission, recording, playback, export, archival, and deletion), the system components involved in each action (e.g., cameras, roadside equipment, video management systems, storage systems, and TMC applications), and the operational context in which those actions occur.

The data action map is used to understand and control where sensitive information may be exposed, duplicated, or persist beyond its intended use. This includes identifying transient storage locations, replication paths, and interfaces where data leaves the CCTV system boundary. The mapping supports implementation of access control, information flow enforcement, encryption, logging, and retention requirements.

Where video or metadata may contain personally identifiable information (PII), the data action map documents whether such processing is intentional, incidental, or prohibited, and ensures that PII handling is limited to explicitly authorized operational or investigative purposes consistent with applicable ITS security and privacy requirements.

CM-14, Signed Components

Responsible Party (M/I): M/I

Justification to Select: Threat "Compromise design, manufacture, and/or distribution of CCTV information system components (including hardware, software, and firmware)" in Table 3, Exploit and Compromise.

Guidance: This control is primarily technical, with organizational oversight. The CCTV system is designed and configured so that critical components such as firmware, software, configuration packages, and updates are cryptographically signed and verified prior to installation, execution, or activation. Signed components provide assurance that code and configuration artifacts originate from an authorized source and have not been altered.

The IOO defines organizational requirements for the use of signed components, including which types of components require signature verification and acceptable cryptographic standards. The manufacturer/vendor implements mechanisms within CCTV devices, video management systems (VMS), and supporting infrastructure to verify digital signatures during boot, update, installation, and runtime execution, and to reject unsigned or improperly signed components.

Signed component enforcement supports secure boot, trusted updates, and supply-chain risk management, and is especially important for field-deployed CCTV devices that may be physically accessible or intermittently connected. Signature verification failures are logged and handled in accordance with configuration management, audit, and incident response procedures.

Risk References and Resources:

NIST SP 800-82(4): The integrity and authenticity of software, firmware, and configuration data are critical for ITS devices, particularly those deployed in remote or physically accessible locations. Digital signatures and integrity checks are commonly used to ensure that only authorized and unmodified components are executed.

CP Family – Contingency Planning

CP-6, Alternate Storage Site

Responsible Party (M/I): I

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

Guidance:

The IOO identifies and documents for alternate storage locations for selected CCTV data necessary to support system recovery, investigations, compliance, or continuity of operations. In an ITS CCTV context, alternate storage is typically limited to critical data such as system configurations, camera and VMS settings, security logs, audit records, certificates, and incident-related video clips, rather than continuous or bulk video streams.

Alternate storage sites may include geographically separated TMC facilities, centralized archival systems, or secure offsite repositories that provide protections appropriate to the sensitivity of the stored data. The IOO ensures that alternate storage locations implement physical and logical controls to commensurate with the data being stored, and that access to alternate storage is restricted and audited.

CP-7, Alternate Processing Site

Responsible Party (M/I): I

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

Guidance:

The IOO determines whether an alternate processing site is required for CCTV system functions that are centrally processed, such as video management, storage management, audit logging, and administrative control typically performed at a Traffic Management Center (TMC) or other backend environment. An alternate processing site, if implemented, supports the continuation or recovery of these centralized functions when the primary processing location is unavailable due to physical disruption, system failure, or other adverse events.

Alternate processing capabilities are generally limited to backend systems (e.g., VMS servers, audit and log processing, configuration management, and selected video retrieval functions) and do not extend to field-deployed CCTV devices, sensors, or camera control elements. Where used, the alternate processing site is geographically distinct and implements physical, environmental, and logical security controls commensurate with the sensitivity of the data and functions being processed, consistent with organizational policy.

Parameter Value(s):

paragraph a.#1 "video feed and audit log storage"
paragraph a.#2 "3 hours"

Risk References and Resources:

NIST SP 800-82⁽⁴⁾: Many site-wide supervisory or optimization servers (i.e., Level 3 and above of the Purdue model) can be supported from an alternate processing site. It is likely not feasible for control systems or field devices, such as sensors or final elements (i.e., Level 1 and 0 of the Purdue model), to be made available from an alternate processing site.

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:

This control is primarily organizational and focuses on the backup of CCTV system information necessary to support recovery and continuity of operations. For CCTV systems, backups typically apply to configuration data, firmware images, certificates and keys, access control settings, audit logs, and incident-related video or metadata, rather than to user information or full system images.

The IOO determines what CCTV system information requires backup, the frequency of backups, and where backups are stored, consistent with the contingency plan. Backup activities are generally performed at centralized locations such as the Traffic Management Center (TMC) or other backend systems. CCTV devices may support this control by providing mechanisms to export or transmit configuration and operational data to authorized backup systems, where feasible.

Parameter Value(s):

paragraph b. "at least weekly or as defined in the contingency plan"
paragraph c. "when created, received, updated, or as defined in the contingency plan"

Risk References and Resources:

ATT&CK for ICS Mitigations / Techniques:

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

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

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: Testing of CCTV system backups is performed by the IOO to verify the integrity, completeness, and usability of backed-up system information. Testing activities focus on configuration data, firmware images, certificates, access control settings, audit logs, and other critical system information required to restore CCTV functionality, rather than full restoration of operational video streams or live camera services.

Testing may be conducted using representative environments, spare equipment, segmented test systems, or controlled sampling of redundant components to avoid disruption to active traffic surveillance operations. Where automated testing mechanisms are desired (e.g., checksum validation, integrity verification, or automated restore validation), the IOO defines and conveys those requirements to the manufacturer/vendor so that the CCTV system supports such capabilities where technically feasible.

Testing frequency, scope, and methods are defined in the contingency plan and account for the operational constraints typical of ITS environments.

Parameter Value(s):

“at least monthly or as defined in the contingency plan”

Risk References and Resources:

NIST SP 800-82⁽⁴⁾: 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 of ITS is often limited to systems with redundancy or spare equipment. In certain cases, sampling will be limited to those redundant systems. Compensating controls may include alternative methods for testing backups, such as hash or checksum validations.

CP-10, System Recovery and Reconstitution

Responsible Party (M/I): M/I

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

Guidance:

The IOO establishes and implements procedures to recover and reconstitute CCTV system components to a known, trusted operational state following disruptions such as power loss, equipment failure, cyber incidents, or physical compromise. Recovery procedures address restoration of firmware, software, configuration settings, cryptographic material, and communications with backend systems such as the Traffic Management Center (TMC).

Recovery and reconstitution activities are based on approved configuration baselines and verified backups maintained by the IOO, typically stored at centralized or protected locations. Reconstitution procedures distinguish between restoring system components to an initial baseline state and restoring previously operational settings, based on operational requirements and safety considerations.

Recovery time objectives are defined by the IOO and reflect the role of CCTV in traffic operations, incident management, and roadway safety.

Parameter Value(s):

“24 hours”

Risk References and Resources:

NIST SP 800-82⁽⁴⁾: 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:

This control is both organizational and technical. The IOO defines the categories of users and systems that require access to the CCTV environment and the corresponding identification and authentication requirements based on role, access method, and operational risk. The manufacturer/vendor implements the technical capability to uniquely identify and authenticate users and systems in accordance with those requirements.

CCTV environments typically support a mix of privileged users (e.g., administrators, maintainers, integrators) and non-privileged users (e.g., operators or viewers). Identification and authentication mechanisms may differ by role and access context. For example, strong authentication is required for administrative access to cameras, VMS platforms, and backend systems, while non-privileged access may be limited to authenticated viewing functions through the VMS.

Authentication is enforced for both local and remote access paths, recognizing that many CCTV devices rely on centralized authentication through a VMS or Traffic Management Center rather than maintaining full identity stores locally. Where local authentication is required (e.g., field maintenance, commissioning, or recovery), mechanisms are designed to balance security with operational needs, including support for controlled shared accounts when individual authentication is infeasible, accompanied by compensating controls such as physical access restrictions and enhanced auditing.

Risk References and Resources:

ATT&CK for ICS Mitigations / Techniques:

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

NIST SP 800-82⁽⁴⁾: When shared accounts are required, compensation 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 control.

ARC-IT Mechanisms:

- Device should require multifactor authentication for the system management actions defined in Notes on Access Control⁽¹³⁾:
 - Install software other than signed software whose signature chains to a verification key whose integrity is protected by hardware on the device.
 - Modify the access control policy specified in AC-3.
 - Modify the information flow control policy specified in AC-4.
 - Define what types of failed authentication attempts are logged for future action as specified in AC-7.
 - The list of auditable activities and the audit log specified in AU-2.
 - Deletion of audit log data as specified in AU-9, except in the case where the audit log has exceeded the allotted storage space.
 - Add or remove root certificates except when this is done via a signed instruction whose signature chains to a verification key whose integrity is protected by hardware on the device.
 - Device may require multifactor authentication for other actions.
- Passwords used in multifactor authentication should meet the requirements specified in IA-5 enhancement 1, authenticator management | password-based authentication.
- Device should require multifactor authentication for the system management actions defined in Notes on Access Control.⁽¹³⁾ See NETWORK ACCESS TO PRIVILEGED ACCOUNTS.
- Device may require multifactor authentication for other locally accessed actions.
- Network access to privileged accounts should be over SSH, which provides replay resistance. NOTE: SSH should use Rivest–Shamir–Adleman (RSA) keys of length 2048 bits or longer or elliptic curve cryptography keys of length 256 bits or longer.
- Device may accept personal identity verification credentials as specified in FIPS 201⁽¹⁷⁾ and supporting guidance documents.
- The information system implements replay-resistant authentication mechanisms for network access to non-privileged accounts.

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 (e.g., administrators, engineers, maintainers, integrators) who perform configuration, management, or security-sensitive actions on CCTV components must be uniquely identified and authenticated using multifactor authentication (MFA), where technically and operationally feasible. MFA combines at least two distinct authentication factors (e.g., knowledge-based, possession-based, or inherence-based factors) appropriate to the access method and operational context.

Remote privileged access to CCTV devices, video management systems (VMS), or associated backend systems (e.g., access via the TMC, maintenance laptops, or backhaul networks) employs MFA to reduce the risk of unauthorized configuration changes, firmware modification, or misuse of camera controls.

For local privileged access performed in the field where remote connectivity is unavailable or unreliable, physical access controls (e.g., locked cabinets, controlled enclosures, hardware keys, or restricted maintenance ports) may serve as one authentication factor when explicitly approved by IOO policy. In such cases, compensating controls such as enhanced auditing, time-limited access, or supervisory procedures are applied to maintain accountability.

Risk References and Resources:

NIST SP 800-82⁽⁴⁾: 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:

For non-privileged users (e.g., operators or field personnel) who access CCTV management interfaces, VMS clients, or supporting applications, the IOO should apply identification and authentication controls commensurate with the risk of the access method and function performed. Non-privileged users must be uniquely identified and authenticated to ensure accountability and session of integrity.

Multifactor authentication (MFA) is recommended for non-privileged accounts when access is performed remotely (e.g., from the TMC network, remote workstations, or mobile devices) or when accessing sensitive information such as recorded video, export functions, or configuration-adjacent capabilities. MFA for non-privileged accounts may combine a password or PIN with a possession-based factor such as a cryptographic token, certificate, or managed device credential.

For local, on-site access where the CCTV component or operator console is physically secured, continuously staffed, and not remotely reachable, MFA may be impractical. In such cases, physical access controls (e.g., locked control rooms, secured cabinets, controlled workstations) may serve as a compensating factor when approved by organizational policy, supplemented by session timeouts, activity logging, and role-based access restrictions.

Risk References and Resources:

NIST SP 800-82⁽⁴⁾: As a compensating control, physical access restrictions may sufficiently represent one authentication factor, provided that the system is not remotely accessible.

IA-3, Device Identification and Authentication

Responsible Party (M/I): M/I

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

Guidance:

The IOO ensures that CCTV system components are uniquely identifiable, and that device-level authentication is enforced where technically feasible prior to establishing trusted communications. Device identification and authentication apply primarily to IP-based components that exchange data over routable networks, including cameras, video encoders, video management systems (VMS), storage systems, and network infrastructure supporting CCTV operations.

Manufacturers and vendors design CCTV devices and associated software to support secure device authentication mechanisms appropriate to their role in the architecture, such as certificate-based authentication, cryptographic device credentials, or mutually authenticated network sessions. Where supported, device authentication is enforced at system boundaries (e.g., camera-to-VMS, camera-to-switch, VMS-to-storage) to prevent unauthorized or rogue devices from participating in video transport, control, or management functions.

The IOO defines which CCTV components require device authentication based on risk, connectivity, and operational role, and establishes device identity lifecycle practices, including secure enrollment, credential provisioning, revocation upon decommissioning, and ongoing monitoring for unauthorized or unknown devices. Device identities are managed in a manner consistent with configuration management and asset inventory controls.

For legacy CCTV components or constrained field devices that cannot natively support cryptographic device authentication, compensating controls are applied. These may include network segmentation, static port assignments, allowlisting at the switch or firewall, physically protected cabling and enclosures, and monitoring unexpected device behavior. Such compensating controls are documented and periodically reviewed as part of the system security plan.

Parameter Value(s):

#1 “all IP cameras, video encoders, network switches, and network attached storage”

#2 “local; remote; and network connection”

Risk References and Resources:

NIST SP 800-82⁽⁴⁾: 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-4, Identifier 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 establishes and maintains processes for the assignment, management, review, and revocation of unique identifiers for all authorized users and system components within the CCTV environment. This includes identifiers for roles such as TMC administrators, operators, maintenance personnel, vendor support accounts, and CCTV devices where applicable.

Identifier management ensures that each user or device can be uniquely distinguished for access control, auditing, and accountability purposes. The IOO defines identifier formats, reuse restrictions, and conditions for identifier deactivation (e.g., personnel transfer, termination, device decommissioning).

Manufacturers implement CCTV system capabilities that support unique identifiers, prevent identifier reuse where prohibited, and ensure identifiers are consistently applied across management interfaces, logs, and access control decisions.

Parameter Value(s):

paragraph a. "Security Administrator"

paragraph d. "At least a year, and upon personnel or device lifecycle changes"

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 establishes and enforces authenticator management requirements for CCTV systems, covering both user authenticators (e.g., administrators, operators, maintenance personnel) and device or system authenticators used for trusted communications with backend systems such as the TMC, VMS, or storage platforms.

For human users, the IOO defines requirements for authenticator strength, rotation, revocation, and compromise handling. Acceptable authenticators may include passwords, hardware tokens, cryptographic certificates, or combinations thereof, consistent with operational constraints and risk. The IOO defines when authenticators must be changed (e.g., suspected compromise, role change, termination) and ensures these events are enforced through policy and audit.

For system and device authentication, manufacturers design CCTV components to support certificate-based authentication using standards-based public key infrastructure (PKI), including X.509 certificates. Where applicable, CCTV devices support integration with a Security Credential Management System (SCMS) or other organizational certificate authority to enable secure enrollment, renewal, revocation, and validation of device credentials. This supports trusted

communications for management interfaces, firmware updates, and system-to-system data exchange.

Manufacturers ensure that authenticators are securely generated, stored, and protected (e.g., using hardware-backed storage where feasible), and that authentication mechanisms operate over secure channels. The IOO manages the lifecycle of authenticators and monitors compliance through logging and review.

Parameter Value(s):

paragraph f. #1 "Every 30 days for password-based authenticators (NIST SP 800-63B⁽⁴⁴⁾), certificate-based authenticators per certificate policy"

#2 Accounts or authenticators are reported as compromised

Risk References and Resources:

NIST SP 800-82⁽⁴⁾: Example compensating controls include physical access control and encapsulating the ITS to provide authentication external to the ITS.

ARC-IT Mechanisms:

- Device should store encrypted hashed-password in a database (only accessible to privileged users) using a strong encryption algorithm.
- Device should enforce password-related security policy (e.g., frequent change, difference between old and new passwords, length, etc.).
- Device should provide a secure mechanism for users to update their password.
- Device should only allow network login attempts over a secure channel.
- Device should require the old password for password reset by a user.
- Device should implement a secure mechanism for "forgot password."
- Device should have a configuration file that describes the list of Security Credential Management System components and how to reach them.
- Device should provide connection to Security Credential Management System components.
- Device should be able to store public key infrastructure-based credentials.
- Device should support communication protocol as specified in Institute of Electrical and Electronics Engineers (IEEE) Standard 1609.2.⁽¹⁹⁾
- Device should support X.509 certificate chain construction.

Standards: NIST SP 800-63B⁽⁴⁴⁾

IA-6, Authentication Feedback

Responsible Party (M/I): M

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

Guidance: CCTV interfaces that require user authentication must obscure authentication input (e.g., passwords or PINs) during entry to prevent disclosure to casual observers. This is particularly

important for operational and maintenance users who may authenticate laptops or terminals in public or semi-public environments such as field cabinets, control rooms, or roadside locations.

Manufacturers design CCTV user interfaces so that authentication feedback does not reveal sensitive information, including masking input characters and avoiding error messages or timing behaviors that distinguish valid from invalid usernames. Where visual feedback cannot be obscured due to interface limitations, operational procedures should require users to physically shield displays during authentication.

Risk References and Resources:

NIST SP 800-82⁽⁴⁾: This control assumes a visual interface that provides feedback about authentication information during the authentication process. When ITS authentication uses an interface that does not support visual feedback (e.g., protocol-based authentication), this control may be tailored out.

ARC-IT Mechanisms: As specified in control; additionally, the system should not leak information about valid vs invalid usernames by errors or login processing time.

IA-7, Cryptographic Module Authentication

Responsible Party (M/I): M

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

Guidance:

Manufacturers design CCTV systems such that access to cryptographic modules and cryptographic functions is restricted to authorized roles and processes. Where CCTV devices implement cryptographic capabilities (e.g., TLS session establishment, certificate storage, firmware verification, or encrypted storage), those capabilities are provided by cryptographic modules that enforce role-based access and separation between cryptographic operations.

Authentication to cryptographic modules is required for any privileged interaction with cryptographic material or functions, such as key generation, key import or export, certificate installation, firmware verification, or cryptographic configuration changes. Authentication mechanisms and role separation must be consistent with the security level of the cryptographic module and applicable standards (e.g., FIPS 140-3).

For most CCTV deployments, cryptographic module authentication is implemented implicitly through authenticated system roles and protected management interfaces rather than through direct operator login to a standalone cryptographic device. Manufacturers ensure that only authorized system processes and privileged users can invoke cryptographic services or access protected key material.

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 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 approved for use with FIPS 140-2⁽¹⁶⁾ at level 2.

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, such as maintenance contractors, integrators, or vendor support personnel, must be uniquely identified and authenticated before being granted access to the CCTV system for diagnostics, maintenance, configuration, or software and firmware updates. These users typically access the system through defined interfaces such as maintenance laptops, remote access gateways, or network-connected management systems.

Manufacturers design CCTV systems to support authentication of non-organizational users using the same underlying mechanisms as organizational users (e.g., unique identifiers, certificates, or credentials), while allowing the IOO to apply additional constraints such as time-limited access, restricted roles, or approval-based activation. Non-organizational accounts are logically distinct from organizational user accounts and are disabled or revoked when access is no longer required.

Authentication requirements for non-organizational users must be enforced regardless of whether access is local or remote and must support accountability and auditing consistent with the IOO’s access control and logging policies.

Risk References and Resources:

NIST SP 800-82⁽⁴⁾: The ITS Discussion for IA-2, Identification and Authentication (organizational users) is applicable for non-organizational users.

IA-9, Service Identification and Authentication

Responsible Party (M/I): M/I

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

Guidance:

The IOO determines which services and system functions within the CCTV architecture require identification and authentication based on their criticality to traffic operations, system integrity, and data protection. These services typically include interfaces that initiate or respond to requests for video streams, control commands, configuration changes, status queries, or data transfers.

Manufacturers design CCTV devices, video management systems (VMS), and associated components so that services authenticate one another before exchanging information or executing

requests. Service identification and authentication may be implemented using mechanisms such as mutually authenticated TLS sessions, certificate-based service identities, or other cryptographically protected service credentials appropriate to the deployment environment.

Service authentication applies regardless of whether services communicate locally (within a cabinet or enclosure) or over a network (e.g., between CCTV devices and the TMC, VMS, or storage systems). Authentication ensures that only authorized services can request video data, issue control commands, or interact with camera controllers, reducing the risk of spoofed services or unauthorized system interactions.

Parameter Value(s):

“Video management services, camera control services, video streaming and playback services, configuration and firmware update services, storage and retrieval services, and monitoring or health-status services associated with the CCTV system.”

Risk References and Resources:

ATT&CK for ICS Mitigations / Techniques:

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

IA-11, Re-authentication

Responsible Party (M/I): M/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 requirements for CCTV systems are defined by the IOO and implemented by the manufacturer/vendor. The IOO identifies the conditions under which users must re-authenticate based on operational risk, role sensitivity, and system exposure. The manufacturer designs CCTV interfaces and management functions to enforce re-authentication when those conditions are met.

CCTV systems may automatically require re-authentication following local or remote session inactivity, session interruption, or other system-detectable events. Conditions that are not directly observable by the CCTV (e.g., role changes, personnel status changes, or system re-categorization) are managed by the IOO through account and access control processes, which may trigger session termination or forced re-authentication through external mechanisms.

Parameter Value(s):

“After 15 minutes of inactivity; upon session interruption or timeout; when authenticators or credentials change; and upon detection of security-relevant events requiring renewed authentication.”

Risk References and Resources:

ARC-IT Mechanisms: Device should provide the ability to force re-authentication when any of the conditions identified in "control" above holds.

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 delivers incident response training tailored to how transportation CCTV is operated and supported, including TMC workflows, field maintenance practices, and vendor-supported components (e.g., camera firmware, VMS, storage). Training covers role-specific responsibilities for detecting, triaging, escalating, and documenting suspected cybersecurity incidents affecting CCTV availability, integrity of video feeds/recordings, unauthorized PTZ/control actions, credential compromise, malicious configuration changes, and abnormal communications between cameras, VMS, storage, and TMC networks.

Training includes: (1) how operators and technicians recognize indicators of compromise in CCTV (e.g., unexpected camera movement, loss-of-video anomalies inconsistent with weather/power events, unauthorized configuration prompts, repeated authentication failures, certificate errors, abnormal outbound connections), (2) how to preserve evidence (e.g., do not reboot/reset unless directed, capture screenshots/log exports, record timestamps/camera IDs), (3) initial containment steps that are operationally safe (e.g., isolate affected camera/VLAN, disable remote access path, revoke vendor account/session, switch to alternate viewing paths if available), and (4) reporting paths and timelines to the IOO security/IT/OT contacts and incident commander.

Parameter Value(s):

paragraph a.1. “Within 72 hours of onboarding or role assignment”

paragraph a.3. “Quarterly (scenario-based tabletop or drills focused on CCTV/VMS/storage/network paths)”

paragraph b. #1 “Quarterly”

#2 “Changes to system roles or responsibilities; onboarding of new CCTV/VMS/storage vendors or major architecture changes; after security incidents; after significant vulnerability disclosures affecting deployed CCTV/VMS components; or changes to IOO incident response procedures”

Risk References and Resources:

NIST SP 800-82⁽⁴⁾: The policy specifically addresses the unique properties and requirements of ITS and the relationship to non-ITS systems.

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 testing for CCTV systems to validate that personnel, procedures, and technical capabilities function as intended during cybersecurity events. Testing focuses on realistic scenarios for transportation CCTV, such as unauthorized access to video feeds, malicious PTZ control, credential compromise, loss of integrity of recorded footage, abnormal communications between cameras, VMS, storage systems, and the TMC, and ransomware or denial-of-service conditions affecting video availability.

Incident response testing is typically performed through structured tabletop exercises, walkthroughs, or limited functional simulations that do not disrupt live traffic operations. Exercises validate detection, reporting, escalation, containment, evidence preservation, coordination with IT/OT and operations staff, and recovery decision-making.

Parameter Value(s):

#1 Quarterly

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 and executes incident handling procedures for CCTV systems that address the full lifecycle of a cybersecurity incident, including detection, analysis, containment, eradication, recovery, and post-incident activities. Incident handling procedures are tailored to the operational role of CCTV in traffic management, incident response, and roadway safety, and prioritize maintaining situational awareness while preventing further compromise.

For CCTV systems, incident handling activities include triaging alerts and anomalies (e.g., unauthorized camera access, unexpected PTZ movement, loss or manipulation of video feeds, abnormal communications with the VMS or storage systems), determining operational impact, and selecting containment actions that do not inadvertently degrade traffic operations or safety. Containment may involve isolating affected cameras or network segments, disabling compromised accounts or services, revoking certificates or credentials, or restricting remote access paths.

Recovery actions focus on restoring CCTV components to a trusted operational state using approved configuration baselines and verified firmware or software images, while preserving logs and other evidence required for forensic analysis or regulatory reporting. The IOO coordinates incident handling activities across operational, IT/OT, and security personnel, and engages manufacturers or vendors as needed for device-specific analysis, remediation guidance, or integrity verification of embedded components.

Lessons learned from incident handling are documented and used to improve detection of capabilities, procedures, training, and coordination with vendors and external partners.

Risk References and Resources:

NIST SP 800-82⁽⁴⁾: As part of the incident handling capability, the organization coordinates with external vendors, integrators, or suppliers as necessary to ensure that they have the capability to address events that are specific to embedded components and devices.

IR-5, Incident Monitoring

Responsible Party (M/I): I

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

Guidance: The IOO monitors CCTV systems during suspected or confirmed cybersecurity incidents to track incident progression, assess operational impact, and support timely containment and recovery decisions. Incident monitoring focuses on observing security-relevant conditions in near real time, including authentication failures, unauthorized access attempts, abnormal PTZ activity, loss or manipulation of video feeds, unexpected configuration changes, and anomalous communications between CCTV devices, VMS, storage systems, and the TMC.

Incident monitoring leverages existing logging, alerting, and monitoring capabilities deployed under the AU and CA families, with elevated attention and correlation during an active incident. The IOO ensures that alerts and relevant telemetry are available to incident responders at the TMC or designated operations center and that monitoring continues through containment and recovery phases to confirm that corrective actions are effective and no residual malicious activity persists.

Risk References and Resources:

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

IR-6, Incident Reporting

Responsible Party (M/I): I

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

Guidance: The IOO establishes requirements for the timely reporting of cybersecurity incidents affecting CCTV systems and ensures that reporting pathways align with operational and security responsibilities. Incident reporting encompasses both system-level incidents (e.g., authentication failures, configuration changes, service disruptions, audit anomalies) and application-level incidents specific to CCTV operation (e.g., camera tampering, unauthorized PTZ movement, loss or manipulation of video streams, abnormal behavior detected by VMS or analytics applications).

Manufacturers and vendors design CCTV devices, VMS, and associated components to support automated generation and transmission of incident reports based on audit and monitoring data. System-level incident reporting leverages audit logs and security events generated under the AU family of controls and supports configurable thresholds and conditions for reporting. Application-level incident reporting is supported where CCTV or VMS applications define misbehavior conditions, with reporting mechanisms that preserve incident data, prioritize reports when storage or connectivity is constrained, and transmit reports securely when connectivity to the TMC or designated incident response authority is available.

The IOO defines the incident response authority, reporting timeframes, and authorized recipients, and ensures that only privileged users can modify reporting conditions or destinations. Incident reports are transmitted using secure communication channels and integrated into the IOO’s broader incident response and escalation processes, including coordination with external entities where required.

Parameter Value(s):

paragraph a. "At least 24 hours"

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

Risk References and Resources:

NIST SP 800-82⁽⁴⁾: The organization should report incidents on a timely basis. The Cybersecurity and Infrastructure Security Agency collaborate with international and private-sector computer emergency response teams to share control systems-related security incidents and mitigation measures

ARC-IT Mechanisms:

ASSUMPTION: There are two different classes of incident: incidents that are common to any networked device, which are handled by non-application-specific mechanisms within the device and are referred to below as "system-level incidents"; and incidents that are specific to activity within a specific cooperative intelligent transport system application, which are detected by application-specific mechanisms and are referred to below as "application-level incidents".

- System-level incidents
 - The device should provide audit report generation functionality as described in AU-1 to AU-12.
 - The device should be configurable to automatically send incident reports based on the generated audit reports to an incident response authority under given conditions.
 - The device should ensure that the conditions under which these incident reports are sent, and the identification and network location information associated with the incident response authority, should only be editable by a privileged user.
- Application-level incidents
 - The application specification should contain performance requirements related to misbehavior reporting, for example:
 - Amount of storage is necessary.
 - How long un-transmitted reports should be stored for.
 - Preservation or deletion of transmitted reports.
 - Prioritization of reports for preservation if the reports exceed the allocated storage.
 - How reports are to be prioritized for transmission to the misbehavior authority when connectivity is available.
 - If a misbehavior is defined for an application, the application should support detecting that misbehavior.
 - The security management services should support receiving misbehavior report payloads and misbehavior reporting configuration information from an application and should support prioritizing which misbehavior reports to send.
 - The device should support transmitting misbehavior reports to a misbehavior authority.

- The device should ensure that the conditions under which these incident reports are sent, and the identification and network location information associated with the incident response authority, should only be editable by a privileged user.

(Assumption: The application specification identifies misbehavior within the context of application activity; for certain applications it is possible that defining misbehavior is not necessary.)

MA Family – Maintenance

MA-2, Controlled Maintenance

Responsible Party (M/I): I

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

Guidance: The IOO establishes and enforces controls over all maintenance activities performed on CCTV system components, including cameras, controllers, VMS, storage devices, and associated network infrastructure. Maintenance activities are authorized in advance, scoped to defined tasks, and executed using approved tools and procedures to prevent unauthorized changes or data exposure.

Controlled maintenance includes managing access to devices during servicing, ensuring that removable storage or equipment leaving the field is sanitized in accordance with organizational policy, and restricting the introduction of unauthorized hardware, firmware, or software. When maintenance is performed off-site or by external parties, the IOO ensures that custody, transport, and return of equipment are documented and that security-relevant data (e.g., video recordings, credentials, certificates, logs) are protected or removed prior to transfer.

Following maintenance, the IOO verifies that the CCTV system is returned to a known, trusted operational state. This includes validating firmware and software integrity, confirming configuration settings, re-enabling required security controls (e.g., encryption, authentication, access enforcement), and ensuring audit logging remains functional. Vendors support this control by providing secure maintenance procedures, integrity verification methods, and documentation necessary to confirm that security controls remain intact after servicing.

Parameter Value(s):

paragraph c. "Maintenance administrators"

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

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

MA-3, Maintenance Tools

Responsible Party (M/I): I

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

Guidance:

The IOO approves and controls the maintenance tools used to support CCTV installation, diagnostics, configuration, firmware updates, and troubleshooting. Maintenance tools include software utilities, scripts, portable devices, and interfaces used to access CCTV components locally (e.g., Ethernet, serial, USB) or remotely through management networks.

The IOO ensures that maintenance tools are authorized, documented, and restricted to trained and approved personnel. Controls include verifying the integrity and origin of tools, limiting tool functionality to approved maintenance activities, and preventing the use of unapproved or ad hoc tools on CCTV components. Where feasible, the IOO requires maintenance tools to authenticate CCTV systems using approved credentials and ensures that tool usage is logged for accountability and post-maintenance review.

Parameter Value(s):

paragraph b. “Quarterly”

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

Responsible Party (M/I): I

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

Guidance: The IOO should implement a process to securely apply software updates and patches to CCTV firmware and software, verifying their authenticity and integrity through cryptographic signatures before deployment to prevent disruptions to real-time traffic messaging. Updates should be tested in a controlled environment and coordinated with the TMC to ensure compatibility and minimize downtime, with all actions logged for audit purposes.

MA-4, Nonlocal Maintenance

Responsible Party (M/I): M/I

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

Guidance: The IOO establishes and enforces policies governing nonlocal (remote) maintenance of CCTV systems, including cameras, controllers, VMS, storage systems, and supporting network components. The IOO determines when remote maintenance is permitted, which roles or vendors are authorized, and the conditions under which access may be granted, based on operational risk and system criticality.

Manufacturers and vendors design CCTV components and management interfaces to support secure nonlocal maintenance by enforcing strong authentication, role-based access, and session monitoring. Remote maintenance access is time-limited, restricted to approved functions, and terminated immediately upon completion of maintenance activities. All nonlocal maintenance sessions are

logged, including user identity, access method, actions performed, and session duration, to support accountability and post-maintenance review.

Where feasible, remote maintenance is performed through controlled access points (e.g., centralized management interfaces or secure gateways) rather than direct connections to individual field devices, and compensating controls are applied when direct remote access is operationally necessary.

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

Responsible Party (M/I): M/I

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

Guidance: The IOO requires that all nonlocal maintenance sessions involving CCTV components are fully logged and subject to review. The IOO defines which maintenance-related activities must be logged and the retention and review requirements and conveys these requirements to the manufacturer/vendor.

Manufacturers and vendors implement mechanisms to generate detailed audit records for remote maintenance activity, enabling the IOO to review sessions for unauthorized access, policy violations, or anomalous behavior. Audit logging focuses on maintenance functions rather than routine operational use of the CCTV system.

Parameter Value(s):

"Remote maintenance session initiation and termination events; authenticated user or service identity; session date and timestamps; session duration; session origination (e.g., vendor network, TMC, maintenance gateway); configuration changes to firmware, software, or system settings; firmware or software upload, update, rollback, and verification attempts; execution of diagnostic or troubleshooting functions; successful and unsuccessful remote maintenance 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 not under asset management” in table 6, Policy and Procedure Vulnerabilities and Predisposing Conditions.

Guidance: The IOO defines requirements for authenticating and isolating nonlocal maintenance sessions used to access CCTV components, including VMS and NAS. The manufacturer/vendor implements mechanisms to ensure remote maintenance sessions use replay-resistant authentication and are logically or physically separated from operational traffic to reduce the risk of lateral movement, unintended interference with live operations, or credential compromise. Maintenance access must be limited to approved channels and disabled when not actively in use.

Parameter Value(s):

paragraph a. "Replay-resistant authentication for remote maintenance sessions; certificate-based or cryptographic authenticators; logical or physical separation of maintenance traffic from

operational video and control traffic; isolation via dedicated management interfaces, VPNs, or maintenance gateways; session termination upon completion of maintenance activities"

Risk References and Resources:

NIST SP 800-82⁽⁴⁾: 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 not under asset management" in table 6, Policy and Procedure Vulnerabilities and Predisposing Conditions.

Guidance: The IOO must obtain maintenance support and spare parts for critical CCTV components, such as cameras, controllers, and network modules. Manufacturers must support the IOO by providing compatible spare parts and detailed maintenance procedures, with documentation ensuring rapid repairs and compliance with ITS standards for integration with the TMC.

Parameter Value(s):

#1 "Cameras, Controllers, Network Modules"

#2 "4 hours"

MP Family – Media Protection

MP-2, Media Access

Responsible Party (M/I): I

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

Guidance: The IOO limits access to CCTV digital media to explicitly authorized individuals based on role and operational needs. Digital media includes removable and embedded storage used for video, logs, configuration data, and firmware. The IOO implements physical protections such as locked field cabinets, secured control room racks, controlled key management, and documented access authorization, and conducts periodic reviews of who is permitted to access media and under what conditions.

The manufacturer/vendor supports this control by designing CCTV components to facilitate media protection, including lockable or tamper-evident storage compartments, the ability to disable unused media ports, logging or alerting when storage media is accessed or removed, and requiring authenticated access before media operations (e.g., export, removal, overwrite) can be performed.

Parameter Value(s):

#1 "Removable media (e.g., USB storage, SD cards, removable drives used for video export, firmware updates, or maintenance)"

#2 "Local device administrators", "Security Administrators"

MP-3, Media Marking

Responsible Party (M/I): I

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

Guidance: This organizational control is particularly relevant in operational environments where physical custody of media changes hands between roles such as maintenance personnel, law enforcement, or external analysts. Given the sensitive nature of the video content, the inadvertent exposure of PII, security incidents, or operational data poses a significant risk. The IOO is responsible for defining a media marking policy that designates when and how media must be labeled.

Parameter Value(s):

paragraph b. #1 "Video footage"

#2 "Physically secured areas", "Areas inaccessible by the general public"

Risk References and Resources:

ARC-IT Mechanisms:

- All data deemed sensitive in nature as classified by the organization will have its intended reader/distribution clearly marked on it.
- Information such as document creator, owner, data, sensitivity rating, and distribution level should all be visible electronically and physically on any sensitive media.
- Watermarks, digital signatures, and tamper-resistant seals are common methods that can be used to mark media.

MP-4, Media Storage

Responsible Party (M/I): M/I

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

Guidance:

The IOO defines and enforces a media marking policy for CCTV-related media to reduce the risk of mishandling, unauthorized disclosure, or inappropriate redistribution of sensitive video and associated metadata. This control is particularly relevant when physical or logical custody of media changes between roles (e.g., field technicians, TMC staff, law enforcement, legal teams, or external analysts).

Media marking requirements apply to both physical and electronic forms of CCTV data and are based on the sensitivity of the content, including the presence of PII, security-relevant imagery, or operational information. Markings are used to clearly communicate handling restrictions, authorized recipients, and distribution limitations at the time media is created, exported, or transferred.

Consistent with ARC-IT mechanisms, markings may be implemented using physical labels, tamper-evident seals, and/or electronic mechanisms such as metadata tags, digital watermarks, or cryptographic signatures. Media markings remain associated with the content for the duration of its lifecycle, including storage, transport, analysis, and archival.

Parameter Value(s):

paragraph a. #1 "Video footage (including exported clips, removable media, and electronically transferred recordings)"

#2 "Physically secured areas", "Areas inaccessible by the general public"

MP-4(2), Media Storage | Automated Restricted Access

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:

This control focuses on **automated, system-enforced restrictions** on access to CCTV media stored on fixed or removable storage. The IOO determines the sensitivity of stored video and metadata and defines access restrictions based on role, operational need, and location (e.g., field cabinet, control room, TMC data center).

The manufacturer/vendor implements technical mechanisms within the CCTV, VMS, and associated storage components (e.g., NVRs, NAS, SANs) to automatically enforce these restrictions without relying on manual procedures. These mechanisms include role-based access controls, authentication checks prior to media access, encryption of stored data, and protections against unauthorized physical or logical access.

Automated controls apply whether the media is accessed locally (e.g., from a field cabinet or maintenance port) or remotely (e.g., via the TMC or approved maintenance connection). Where removable media is supported, the system enforces access restrictions at the time of insertion, mounting, or export to prevent unauthorized viewing, copying, or modification.

Parameter Value(s):

#1 "Role-based access enforcement for stored video and metadata; authentication required prior to media access; automated tamper detection and alerting for storage access attempts"

MP-7, Media Use

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: This control governs how CCTV media may be used once accessed, including viewing, copying, exporting, analysis, and sharing of video and associated metadata. Media use is restricted based on operational need, legal requirements, and privacy considerations, including limitations on secondary use, redistribution, and playback outside approved environments.

CCTV systems, associated video management systems, and storage components enforce media use restrictions through technical and administrative controls. These include role-based access controls, encryption of stored and exported video, binding of exported media to authorized platforms or devices, watermarking or labeling of exported footage, and logging of all media access, export, and playback actions.

Restrictions apply to fixed and removable media and to all exported CCTV content, including footage used for incident investigation, maintenance analysis, legal proceedings, or information sharing with external entities.

Parameter Value(s):

paragraph a. #1 Restrict

#2 "CCTV video footage and associated video metadata"

#3 "CCTV cameras, video management systems (VMS), network video recorders (NVR/DVR), centralized storage systems, and approved playback or analysis workstations"

#4 "role-based access control, approved playback environments, encryption of exported media, watermarking or labeling of footage, platform or device binding for exported video, and audit logging of media access and export actions"

Risk References and Resources:

ATT&CK for ICS Mitigations / Techniques:

- M0934 / T0847

MP-8, Media Downgrading

Responsible Party (M/I): I

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

Guidance: This organizational control ensures information stored on digital media is properly sanitized before its classification is downgraded, or the media is released. This includes ensuring that any sensitive content is removed, masked, or redacted to prevent exposure. The IOO is responsible for establishing policies and procedures governing the review and sanitization of CCTV footage prior to external sharing. These policies should define what constitutes sensitive information, who is authorized to perform downgrading or redaction, and how the review process must be documented. The manufacturer/vendor supports this control by enabling export and editing features that facilitate content downgrading.

Parameter Value(s):

Paragraph a. "Documented procedures for reviewing, sanitizing, masking, redacting, or otherwise modifying CCTV video and associated metadata prior to downgrading its classification, including approval and documentation requirements."

Paragraph c. "CCTV video footage and associated metadata exported or released for public disclosure, training, research, legal proceedings, or sharing with external entities."

PE Family – Physical and Environmental Protection

PE-2, Physical Access Authorizations

Responsible Party (M/I): I

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

Guidance: The IOO defines, documents, and enforces physical access authorizations for all CCTV system components, including field-deployed cameras, pole-mounted cabinets, roadside enclosures, control room equipment, and backend systems supporting video storage and management. Authorized personnel are explicitly designated based on role and operational need, and access is limited to those individuals whose duties require physical interaction with the equipment.

For field-deployed CCTV devices, physical access authorizations govern who may access camera housings, pole cabinets, junction boxes, and any embedded maintenance or diagnostic interfaces. Authorization mechanisms may include keyed locks, electronic access controls, maintenance credentials, or work order–based authorization processes managed by the IOO.

Physical access authorizations also apply to facilities and systems supporting CCTV operations, including Traffic Management Centers, video management systems, storage infrastructure, and network equipment. Access to these systems is restricted consistent with their role in storing, processing, or transmitting CCTV data.

The IOO reviews physical access authorizations periodically and updates them to reflect personnel changes, role changes, and evolving operational requirements

Parameters:

Paragraph c. “at least annually”

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

Responsible Party (M/I): I

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

Guidance: The IOO authorizes physical access to CCTV system components based on defined positions or roles, rather than individual discretion or ad hoc need. Only personnel in approved roles such as installers, field maintainers, system administrators, or other designated operational staff are permitted physical access to CCTV devices and supporting infrastructure.

Role-based physical access authorizations apply to all components where physical interaction could enable configuration changes, diagnostics, firmware updates, media access, or network connectivity. This includes, but is not limited to, camera housings, pole-mounted cabinets, roadside enclosures, local network interfaces, and any physically accessible components of supporting systems such as VMS, NAS, SAN, or other storage or networking equipment.

Physical access granted by role is aligned with job responsibilities and least privilege principles, and is reviewed and updated as roles, personnel assignments, or operational needs change. Possession of physical access does not imply unrestricted logical access; logical access controls remain enforced separately.

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:

Physical access controls for CCTV systems are implemented at the device and enclosure level rather than through traditional facility controls. CCTV cameras, pole-mounted cabinets, roadside enclosures, and associated field-deployed components are protected using tamper-resistant housings, locks, and mounting mechanisms appropriate to their outdoor and unattended operating environments.

The IOO establishes policies governing who may physically access CCTV equipment and under what conditions, including requirements for key management, inspection, and periodic review. Physical access controls are designed to prevent unauthorized opening, removal, or manipulation of camera housings, storage compartments, network interfaces, and maintenance ports.

CCTV devices and associated field hardware incorporate physical protection features such as lockable housings, sealed or tamper-evident enclosures, and mechanisms to detect or deter unauthorized access. Where feasible, physical access events are logged or otherwise documented to support accountability and incident investigation. Emergency access considerations are addressed through defined procedures that balance safety, operational continuity, and security.

Parameter Value(s):

Paragraph a. “IP-based and analog CCTV cameras, dome housings, roadside cabinets, physical network switches, video management devices, and attached storage components”

Paragraph a.2. “Integrated keyed locks, hardened fasteners, or externally mounted padlocks appropriate to the deployment environment”

Paragraph f. #2 “at least annually, or upon personnel transfer, role change, or termination involving physical access privileges”

Paragraph g. “at least annually”

Risk References and Resources:

NIST SP 800-82⁽⁴⁾: 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: Physical access to CCTV system components that provide control, recording, or storage functions must be restricted to authorized personnel. For IP-based CCTV deployments, this includes protecting network video recorders (NVRs), video management system (VMS) servers, network switches, and attached storage from unauthorized physical access. For analog or hybrid systems, digital video recorders (DVRs), multiplexers, and associated storage devices require equivalent protection.

Physical safeguards are applied to field-deployed components (e.g., camera housings, roadside cabinets) as well as centralized or remote components (e.g., control rooms, equipment racks, storage locations). Controls may include locked enclosures, secured cabinets, controlled access rooms, and documented key or access device management. The IOO ensures that physical access protections align with operational needs, safety requirements, and the sensitivity of the video and system functions supported by each component.

Parameter Value(s):

Paragraph a. “physical network switches, video management devices (NVRs, DVRs, VMS servers), attached storage systems, and CCTV camera housings or enclosures”

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: CCTV system components deployed in the field or in unsecured or semi-public locations are protected by lockable casings to prevent unauthorized physical access, tampering, or removal. Lockable casings apply to camera housings mounted on poles, structures, or buildings, as well as to recording and processing components located in roadside cabinets, control rooms, or equipment racks. The use of lockable casings supports defense-in-depth by complementing physical access authorization, monitoring, and maintenance controls.

Locking mechanisms are appropriate to the deployment environment and may include integrated keyed locks, hardened fasteners, or enclosure designs that require specialized tools to open. Access to lockable casings is limited to authorized roles in accordance with established physical access authorization policies.

Parameter Value(s):

“CCTV cameras, digital video recorders (DVRs), network video recorders (NVRs), and field-deployed CCTV equipment enclosures”

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.

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

Guidance: CCTV system components deployed in the field or within accessible enclosures incorporate tamper protection and tamper detection measures to safeguard against unauthorized modification, component substitution, or insertion of malicious hardware. Tamper protections apply to camera housings, roadside cabinets, and any enclosure containing recording, processing, or storage components.

Tamper protection mechanisms are implemented to both prevent unauthorized access and provide detectable evidence of attempted or successful tampering. These mechanisms support timely incident detection and response and are integrated with physical access controls, maintenance procedures, and monitoring processes. Tamper events affecting critical components are treated as security-relevant events and handled in accordance with incident response and audit requirements.

Parameter Value(s):

#1 "Anti-tamper coatings", "Tamper-detection seals", "Disabling media ports"

#2 "prevent and detect"

#3 "key/critical components (e.g., NVR, DVR, DAS)"

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: CCTV transmission paths are frequently exposed due to roadside, pole-mounted, or cabinet-based deployments and are therefore subject to physical tampering, interception, or accidental disruption. Physical access controls are applied to protect transmission media and connection points that carry video, control, and management of traffic between cameras, storage devices, and backend systems.

Physical protections focus on limiting unauthorized physical contact with transmission interfaces and cabling rather than inspecting or filtering traffic content. Controls include securing cable runs within conduit, protecting splice points and junction boxes, restricting access to wiring compartments and cabinets, and preventing unauthorized attachment to physical network interfaces. Transmission access controls are coordinated with physical access authorization and tamper protection measures to reduce the risk of signal interception, insertion of rogue devices, or service disruption.

Parameters:

1st PV: "CCTV's media connectors"

Risk References and Resources:

ARC-IT Mechanisms:

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

PE-6, Monitoring Physical Access

Responsible Party (M/I): M/I

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

Guidance: Physical access monitoring for CCTV systems focuses on detecting and recording unauthorized access to field-deployed equipment installed in publicly accessible environments, such as poles, gantries, cabinets, and roadside enclosures. Unlike traditional facilities, these deployments may not support continuous human monitoring or formal entry logs. Instead, monitoring is achieved through technical means that detect physical interaction with protected components.

Physical access monitoring includes detecting enclosure openings, removal or displacement of equipment, power interruptions inconsistent with normal operations, loss of video signal indicative of tampering, and other conditions suggesting unauthorized physical access. These events support timely awareness and response by operations or security personnel and may be correlated with system health, availability, and security monitoring to distinguish accidental damage from intentional interference.

Monitoring mechanisms support periodic review and near-real-time notification, consistent with operational constraints and the criticality of the CCTV system to traffic operations and roadway safety.

Parameter Value(s):

Paragraph b. #1 "at least monthly "

#2 "unauthorized access attempts, camera outages, or facility entry anomalies"

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:

Power equipment and cabling supporting CCTV systems must be protected against tampering, accidental damage, and unauthorized physical access, particularly in roadside and other publicly accessible environments. CCTV enclosures protect internal power components, cabling, and any integrated battery or uninterruptible power elements used to support continued operation or graceful shutdown.

External power equipment and cabling that support CCTV operations such as conduit runs, junction boxes, and power distribution components are identified and protected using physical safeguards appropriate to the deployment environment. Protection measures account for environmental exposure, accessibility, and the operational importance of maintaining continuous video capture and transmission.

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: CCTV systems that support traffic operations and incident management must maintain operation during power disruptions consistent with their operational criticality. Emergency power capabilities may include connection to roadway power backup systems, cabinet-level battery backups, or centralized emergency power supporting associated management and storage systems.

Parameter Value(s):

"Transition of the system to emergency power and continued system operation without delay"

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: CCTV components are typically deployed outdoors or in roadside environments and must be engineered to operate reliably under expected environmental extremes. Environmental protection is achieved primarily through hardened equipment design rather than building-based controls.

CCTV cameras, dome housings, field cabinets, and associated components are designed and installed to tolerate applicable environmental conditions, including temperature extremes, humidity, precipitation, dust, vibration, barometric pressure, and ultraviolet exposure. Environmental tolerance requirements are defined by the IOO and reflected in applicable specifications, standards, and procurement requirements for CCTV components to ensure continuous and reliable operation.

Parameter Value(s):

Paragraph b. “continuously”

Risk References and Resources:

NIST SP 800-82⁽⁴⁾: ITS can operate in extreme environments and both interior and exterior locations. For a specific ITS, the temperature and humidity design and operational parameters dictate the performance specifications. As ITS and information technology become interconnected and the network provides connectivity across the hybrid domain, power circuits, distribution closets, routers, and switches that support fire protection and life safety systems must be maintained at the proper temperature and humidity. When environmental controls cannot be implemented, use hardware that is engineered to withstand the unique environmental hazards.

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

Responsible Party (M/I): M/I

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

Guidance: Environmental monitoring for CCTV systems focuses on detecting conditions that could degrade availability, integrity, or safety rather than maintaining controlled indoor environments. CCTV components deployed in dome housings, field cabinets, or roadside enclosures support monitoring of environmental conditions such as temperature extremes, moisture intrusion, loss of enclosure integrity, or power anomalies.

When supported by the system design, environmental alarms and notifications are generated upon detection of abnormal or out-of-tolerance conditions and reported to authorized personnel for timely response. Environmental monitoring may be integrated with device health monitoring, tamper detection, or centralized management systems used by the IOO to support operational awareness and incident response.

Parameter Value(s):

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

PE-21, Electromagnetic Pulse Protection

Responsible Party (M/I): M/I

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

Guidance: Electromagnetic interference, including electromagnetic pulse (EMP), lightning-induced surges, static discharge, and voltage irregularities, can disrupt or damage roadside CCTV equipment. For transportation of CCTV deployments, protection focuses on resilience to realistic electromagnetic and electrical disturbances rather than military-grade EMP scenarios.

CCTV components and enclosures incorporate appropriate protective measures such as electrical grounding, surge suppression, shielding, and hardened power interfaces to reduce susceptibility to electromagnetic effects. Protection mechanisms are applied consistently across cameras, recording devices, and associated field equipment to support system availability and prevent data corruption or loss.

Parameter Value(s):

#1 "Routine data backups", "Shielding"

#2 "CCTV cameras, DVRs, and network video recorders (NVRs)"

Risk References and Resources:

NIST SP 800-82: Organizations that manage ITS equipment may choose to utilize EMP protection to prevent adversarial or environmental electromagnetic threats. Organizations may select to follow National Coordinating Center for Communications (NCC) guidelines on EM pulse protection.

PL Family – Planning

PL-2, System Security and Privacy Plans

Responsible Party (M/I): I

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

Guidance:

This is an organizational control that establishes the foundation for managing cybersecurity and privacy risk for transportation of CCTV systems. The IOO develops, documents, and maintains a system security and privacy plan that describes how security and privacy requirements are implemented across the CCTV architecture, including cameras, field cabinets, communications links, VMS, storage components, and interfaces with TMCs.

The plan documents system boundaries, roles and responsibilities, applicable security controls, data handling and privacy protections for video and metadata, and dependencies on external or supporting systems. It also describes how security-relevant activities such as logging, monitoring, incident response, maintenance, and information sharing are coordinated across system components. The plan is kept current to reflect system changes, operational updates, and evolving risk conditions.

Parameter Value(s):

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

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

paragraph c. "At least Annually"

Risk References and Resources:

NIST SP 800-82⁽⁴⁾: 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: This is an organizational control that documents how the CCTV system is intended to operate throughout its lifecycle, with explicit consideration of security and privacy. The Infrastructure Owner and Operator (IOO) develop and maintains a concept of operations that describes how CCTV capabilities are used to support traffic operations, incident management, and situational awareness while managing cybersecurity and privacy risks.

The concept of operations addresses operational context and assumptions, including camera placement and coverage, user roles and responsibilities, access to live and recorded video,

interaction with video management systems (VMS) and storage platforms, and coordination with Traffic Management Centers (TMCs). It also documents how security controls are applied during normal operations, maintenance activities, incident response, and information sharing, ensuring that operational practices align with established security and privacy requirements.

Parameter Value(s):

paragraph b. "Annually"

Risk References and Resources:

NIST SP 800-82⁽⁴⁾: 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.

PL-8, Security and Privacy Architectures

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, documents, and maintains a security and privacy architecture for the CCTV system that describes how confidentiality, integrity, and availability are preserved across the system lifecycle. The architecture defines system boundaries, trust zones, and information flows among cameras, field devices, communications infrastructure, storage systems, video management systems, and the TMC.

The security and privacy architecture should be informed by established ITS architectural frameworks, such as ARC-IT, to ensure consistency with recognized system viewpoints, service packages, and interface definitions. ARC-IT can be used to identify CCTV-related system elements, external system interfaces, and data flows, providing a structured foundation for applying security and privacy controls to video, metadata, and management of communications.

The architecture addresses protection of video data and management interfaces, including considerations for external system connections, centralized storage, remote access, and monitoring functions. Where CCTV operations may capture individuals or sensitive activity, the architecture documents how privacy risks are identified and managed. The security and privacy architecture is reviewed and updated as the system evolves to reflect changes in technology, connectivity, or operational use.

Parameter Value(s):

Paragraph b. "Annually"

PM Family – Program Management

PM-5, System Inventory

Responsible Party (M/I): M/I

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

Guidance: The IOO develops and maintains a comprehensive inventory of all CCTV system components to support program-level risk management, oversight, and accountability. The inventory includes hardware components (e.g., cameras, encoders, storage devices such as NVRs/NAS), software applications, and firmware versions associated with CCTV operations. The inventory supports identification of authorized assets, detection of unauthorized or obsolete components, and coordination of vulnerability management, maintenance, and lifecycle planning activities across the CCTV program.

The system inventory is maintained at a level appropriate for program management and complements, but does not replace, detailed configuration inventories maintained under the Configuration Management family. Inventory records are updated to reflect system changes and are reviewed periodically to ensure continued accuracy.

Parameter Value(s):

Paragraph b. "Quarterly"

PM-9, Risk Management Strategy

Responsible Party (M/I): M/I

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

Guidance: The IOO establishes and maintains a risk management strategy for the CCTV program that identifies, assesses, and prioritizes risks to the confidentiality, integrity, and availability of video data and supporting systems. The strategy defines how cybersecurity risks are framed, evaluated, accepted, mitigated, or monitored over time, taking into account the operational role of CCTV in traffic management, incident response, and roadway safety.

The risk management strategy aligns CCTV risk decisions with broader ITS and TMC risk management practices and informs system design choices, operational procedures, maintenance activities, and investment priorities. Risk considerations include, but are not limited to, exposure of video feeds, unauthorized access to cameras or storage, firmware and supply chain risks, physical compromise of roadside assets, and dependencies on external systems such as VMS, storage platforms, and communications infrastructure.

Risk assessments and mitigation priorities are reviewed periodically and updated in response to significant system changes, newly identified threats or vulnerabilities, or operational incidents.

Parameter Value(s):

"Annually"

PM-30, Supply Chain Risk Management Strategy

Responsible Party (M/I): M/I

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

Guidance: The IOO establishes and maintains a supply chain risk management strategy for the CCTV program to identify, assess, and manage risks associated with the sourcing, development, integration, and sustainment of system components. The strategy addresses risks related to hardware, firmware, software, and supporting services throughout the system lifecycle, including procurement, installation, maintenance, and replacement.

Supply chain risk considerations include component provenance, use of trusted suppliers, firmware and software integrity, secure update mechanisms, lifecycle support expectations, and environmental and operational suitability for roadside deployment. The strategy informs procurement decisions, contract requirements, acceptance testing, and ongoing monitoring activities to reduce the likelihood of counterfeit, tampered, unsupported, or vulnerable components being introduced into the CCTV environment.

The supply chain risk management strategy is reviewed and updated periodically to account for changes in the threat landscape, vendor relationships, system architecture, or operational requirements.

Parameter Value(s):

"Annually"

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

Responsible Party (M/I): M/I

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

Guidance: The IOO identifies, evaluates, and approves suppliers for critical or mission-essential CCTV components based on their ability to meet defined security, reliability, lifecycle support, and operational requirements. Critical components may include cameras, encoders, communications interfaces, storage devices, and any elements that directly affect video availability, integrity, or system control.

Supplier evaluation considers factors such as component provenance, firmware and software integrity practices, vulnerability disclosure and patching processes, support for secure configuration and updates, and long-term availability of replacement parts. The IOO incorporates these considerations into procurement criteria, acceptance testing, and ongoing operational oversight to reduce the risk of introducing compromised, unsupported, or untrusted components into the CCTV environment.

Supplier trust decisions and any associated risk acceptance are documented and reviewed periodically as part of the broader supply chain risk management strategy.

PS Family – Personnel Security

PS-3, Personnel Screening

Responsible Party (M/I): I

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

Guidance: The IOO establishes and enforces personnel screening requirements for individuals with authorized access to CCTV systems, including access to live video feeds, recorded footage, configuration interfaces, or supporting systems such as VMS and storage platforms. Screening requirements are commensurate with the level of access granted and the sensitivity of the information exposed, recognizing that CCTV systems may reveal operational details, security posture, or personally identifiable information.

Screening applies to personnel in operational, administrative, maintenance, and security roles and is conducted prior to granting access and periodically thereafter, based on organizational policy and risk tolerance.

Parameter Value(s):

Paragraph b. "regularly"

PS-4, Personnel Termination

Responsible Party (M/I): I

Justification to Select: Threat "Exploit vulnerabilities on internal organizational information systems" in Table 3, Exploit and Compromise.

Guidance: The IOO ensures that when personnel are terminated, transferred, or otherwise no longer require access to CCTV systems, all logical and physical access is promptly revoked. This includes disabling user accounts, revoking credentials and certificates, recovering keys or access devices, and removing access to CCTV management interfaces, video feeds, and stored footage.

Termination procedures are coordinated with system administrators and security personnel to ensure access revocation occurs within defined timeframes and that no residual access remains.

Parameters:

Paragraph a. "24 hours"

Paragraph c. "Non-disclosure agreements"

PS-6, Access Agreements

Responsible Party (M/I): I

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

Guidance: The IOO requires all personnel with authorized access to CCTV systems to formally acknowledge and comply with documented access agreements prior to being granted access. These agreements define acceptable use, confidentiality obligations, privacy considerations, restrictions on disclosure or redistribution of video content, and consequences for misuse or policy violations.

Access agreements apply to all roles, including operators, administrators, maintainers, and contractors, and are reviewed and reaffirmed periodically to ensure continued awareness of responsibilities associated with CCTV access.

Parameter Value(s):

Paragraph b. "annually"

Paragraph c2. "annually"

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 establishes and maintains a risk assessment process for the CCTV system to identify threats, vulnerabilities, likelihoods, and potential impacts on system confidentiality, integrity, availability, and operational safety. Risk assessments consider the full CCTV architecture, including field devices, communications paths, management interfaces, storage systems, and integration with TMC operations.

Risk assessments are conducted throughout the system lifecycle. During design and acquisition, risk information provided by manufacturers, integrators, and suppliers is used to inform architectural and security decisions. Once deployed, the IOO performs ongoing risk assessments to account for changes in system configuration, threat environment, operational use, and interconnections with other ITS systems. Risk assessments may be qualitative or quantitative based on organizational capability and resource constraints, provided the method supports defensible, risk-based decision-making.

Parameters:

Paragraph d "at least annually"

Paragraph f. "at least annually"

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

Responsible Party (M/I): 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 includes supply chain considerations as part of its overall CCTV risk assessment activities, evaluating risks associated with sourcing, development, delivery, and maintenance of hardware, firmware, and software components. This includes assessing risks related to component provenance, vendor trustworthiness, update mechanisms, and dependency on third-party services.

Supply chain risk information obtained during procurement and system development is used to inform supplier selection, architectural decisions, and compensating controls. Supply chain risks are reassessed over time to account for changes in vendors, component lifecycles, discovered vulnerabilities, or emerging threats that could affect the integrity or reliability of CCTV system components.

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 and maintains a vulnerability scanning and monitoring approach for the CCTV system that is appropriate for its operational role, deployment environment, and safety constraints. Vulnerability scanning encompasses the identification of known weaknesses in hardware, firmware, software, configurations, and exposed services across CCTV field devices, management interfaces, communications paths, and supporting systems such as VMS and storage platforms. Once deployed, the IOO conducts vulnerability monitoring using methods suitable for operational technology environments. Active scanning is used selectively and only when it does not risk disrupting video capture, traffic operations, or roadway safety. Passive techniques—such as configuration review, asset inventory correlation, log analysis, and comparison against public vulnerability advisories (e.g., CVEs, vendor advisories)—are used to maintain situational awareness without impacting availability. When active scanning is required, it is scheduled during planned maintenance windows or performed against replicated or test environments that mirror production configurations. Vulnerability scanning activities account for the unique characteristics of CCTV systems, including non-routable interfaces, embedded operating systems, limited computer resources, and continuous operational requirements. Findings are documented, prioritized based on risk and operational impact, and tracked through remediation, mitigation, or risk acceptance decisions.

Risk References and Resources:

ATT&CK for ICS Mitigations / Techniques:

- M0916 / T0819

NIST SP 800-82⁽⁴⁾: 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, a 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 and Infrastructure Security Agency advisories, NIST National Vulnerability Database⁽²¹⁾). Production may need to be taken offline before active scans can be conducted. Scans are scheduled to occur during planned OT outages whenever possible. If vulnerability scanning tools are used on adjacent non-OT networks, extra care is taken to ensure that they do not mistakenly scan the OT 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 investigating application patch levels, device configuration, exposed services, and known vulnerabilities shall occur at regular intervals (daily, weekly)
- Device scanning tool will maintain regular security signature updates of its own.
- The device will report on security weaknesses so that 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 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 OWASP-Top 10 vulnerabilities)
- Web applications shall also 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 of 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(6), Vulnerability Scanning | Automated Trend Analysis

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 establishes processes to analyze vulnerability data over time to identify trends, recurring weaknesses, and systemic issues affecting the CCTV environment. This includes comparing results from successive scans, advisories, configuration reviews, and vendor disclosures to detect patterns such as unpatched components, persistent misconfigurations, or recurring exposure of management services.

Trend analysis supports risk-based decision-making by highlighting areas where vulnerabilities are increasing in frequency or severity, where compensating controls are relied upon long-term, or where architectural changes may be warranted. Results are used to inform prioritization of remediation activities, updates to configuration baselines, procurement decisions, and improvements to security monitoring and incident response practices.

RA-8, Privacy Impact Assessments

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 conducts privacy impact assessments for the CCTV system to identify and evaluate risks associated with the collection, processing, storage, and sharing of video and associated metadata that may contain personally identifiable information (PII), such as faces, vehicle identifiers, or location and movement patterns. Privacy impact assessments consider the full CCTV data lifecycle, including camera placement, field of view, recording policies, retention periods, access controls, and information sharing with external entities.

Assessments are used to determine whether the CCTV system collects more information than is operationally necessary and to identify mitigations that reduce privacy risk while preserving traffic operations and public safety objectives. Mitigations may include camera placement and orientation controls, masking or redaction of sensitive areas, role-based access restrictions, retention limits, and controlled export or sharing of footage.

The CCTV system supports privacy impact assessments by providing configurable technical features that enable privacy protections to be applied and adjusted as operational needs, legal requirements, or risk conditions change. Documentation and system artifacts necessary to understand data flows, storage locations, and access paths are maintained to support repeatable and auditable privacy assessments over time.

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, documents, and maintains cybersecurity requirements for the CCTV system as part of the acquisition process. These requirements address security objectives across the system lifecycle, including design, development, delivery, installation, and sustainment. Acquisition documentation reflects the IOO’s risk tolerance and operational priorities, recognizing that some security properties (e.g., secure defaults, configuration transparency, and supportability) may be more critical than others depending on deployment context.

Cybersecurity requirements are integrated into acquisition artifacts such as solicitations, contracts, and acceptance criteria to ensure that security is addressed early and consistently rather than retrofitted after deployment. The IOO may select additional acquisition-related control enhancements to increase assurance where higher risk or system criticality warrants it.

Risk References and Resources:

NIST SP 800-82⁽⁴⁾: 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 acquisition process includes requirements for sufficient design and implementation of transparency to support security review, configuration, operation, and long-term maintenance of the CCTV system. Information provided supports the IOO’s ability to understand security-relevant system behavior, validate implemented controls, and assess operational risk.

Parameter Value(s):

#1. "Security-relevant external system interfaces; high-level design; low-level design;

source code and hardware schematics"

#3. "At the function-level with encryption module specifications and access control matrices

Risk References and Resources:

NIST SP 800-82⁽⁴⁾: 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 acquisition process specifies secure baseline configurations for CCTV system components. Systems are delivered with security controls enabled by default and configured to minimize exposure prior to operational deployment. Secure configuration expectations include disabling unused functions, ports, protocols, and services; enforcing credential initialization controls; enabling encrypted communications; and restricting wireless capabilities unless explicitly required.

Baseline configurations are documented to support validation, operational use, and future configuration management activities.

Parameter Value(s):

Paragraph a. the U.S. Government Configuration Baseline (USGCB), Security Technical Implementation Guides (STIGs), and any limitations on functions, ports, protocols, and services

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

Responsible Party (M/I): M/I

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

Guidance: The acquisition process defines which system functions, ports, protocols (including version constraints), and services are permitted for CCTV operation. These definitions reflect operational requirements and the principle of least functionality, ensuring that only capabilities necessary for video capture, transmission, management, and maintenance are enabled.

This information is used to establish configuration baselines, support security testing and validation, and inform ongoing monitoring and vulnerability management activities.

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: System documentation is maintained for all CCTV components and any externally connected systems, including NVRs, DVRs, VMS platforms, and external storage devices. Documentation includes architecture diagrams, data flows, interface descriptions, authentication and authorization mechanisms, encryption usage, logging behavior, and operational dependencies. Documentation is written at a level sufficient for security oversight, configuration management, incident response, and continuity activities, and is kept current as system components or integrations change.

Parameter Value(s):

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

SA-8, Security and Privacy Engineering Principles

Responsible Party (M/I): M/I

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

Guidance: Security and privacy engineering principles are applied throughout the CCTV system design and acquisition lifecycle. System architecture and component selection reflect least privilege and separation of duties for users, services, and devices. Secure defaults are used for configurations, services, and interfaces, minimizing exposure prior to deployment. Defense-in-depth mechanisms are employed across physical, network, application, and management layers. Systems fail securely by default, preserving confidentiality and integrity during faults or degraded states. Privacy-by-design

principles are incorporated where video data may contain PII, including minimization of collection, transparency of use, and controls that support lawful and limited disclosure.

Parameter Value(s):

"least privilege, secure defaults, defense in depth, fail securely, complete mediation, separation of duties, and privacy by design (minimization, transparency, and individual participation)"

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: When the CCTV system relies on external system services, the IOO defines security and operational requirements governing those services. External services are approved only when they meet defined security controls for authentication, encryption, access control, and integrity protection. Ongoing assurance mechanisms are established to monitor the security posture of external services and to detect deviations that could affect CCTV confidentiality, integrity, or availability.

Parameter Value(s):

paragraph a. "mutual TLS 1.3, FIPS 140-3 validated encryption for stored video, role-based access controls, and tamper-evident logging"

paragraph c. "monthly security posture reports, automated certificate and firmware signature validation, annual third-party penetration testing, and real-time SIEM alerts for anomalous traffic"

SA-9(2), External System Services | Identification of 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: All ports, protocols, services, and functions used to support CCTV external connections are explicitly identified, documented, and approved. This includes interfaces used by network switches, recording systems, storage devices, and management services. Only those ports and protocols required for operational functionality are permitted, and unused or unsupported interfaces are disabled or blocked. This identification supports configuration management, vulnerability scanning, and incident response activities.

Parameter Value(s):

IP-based systems: NVR, NAS; analog systems: DAS.

SA-10, Developer Configuration Management

Responsible Party (M/I): I

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

Guidance: Developer configuration management ensures that CCTV hardware, firmware, and software are built, maintained, and delivered in a controlled and traceable manner. For CCTV

systems, this includes camera firmware, embedded operating systems, device drivers, video encoding libraries, network services, management interfaces, and any externally integrated software components (e.g., VMS agents or storage connectors).

Configuration management practices cover the full lifecycle of CCTV components, from design and development through deployment, update, and retirement. Configuration items subject to control include source code, firmware images, build scripts, configuration templates, cryptographic material, and security-relevant parameters such as enabled services, ports, protocols, and authentication mechanisms. Changes to these items are tracked, versioned, and auditable, ensuring that security fixes are not inadvertently removed and that deployed systems can be reliably compared against known baselines.

Parameter Value(s):

paragraph a. "design, development, implementation, operation, and disposal"

paragraph b. "all software, firmware, hardware design artifacts, build artifacts, and security-relevant configuration items under configuration management"

paragraph e. "CISO, System Administrator, and System Owner"

Risk References and Resources:

NIST SP 800-82⁽⁴⁾: 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 Verification

Responsible Party (M/I): M/I

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

Guidance: Software and firmware integrity verification ensures that CCTV components execute only authorized and unmodified code. Firmware images, operating system components, and application software are verified against known-good values prior to execution and during update operations. Integrity verification mechanisms include cryptographic hashes, digital signatures, or secure boot processes that prevent unauthorized or corrupted software from running on the device.

Software and firmware updates are authenticated before installation, ensuring updates originate from a trusted source and have not been altered in transit. This is especially critical for roadside-deployed CCTV devices where physical access is limited and compromise may not be immediately observable.

Integrity verification supports reliable patching, forensic validation, and recovery following security incidents.

Risk References and Resources:

NIST SP 800-82⁽⁴⁾: 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: Vulnerability “Hardware, firmware, and software are not under configuration management” in Table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: Hardware integrity verification ensures that CCTV devices operate only with authorized and untampered hardware components. CCTV systems are designed to detect or prevent the use of unauthorized hardware modifications that could compromise device behavior, such as altered processors, storage modules, debug interfaces, or communication components.

For CCTV deployments in publicly accessible environments, this includes mechanisms to verify hardware identity at startup, detect unexpected changes to critical components, and prevent operation when integrity checks fail. Hardware integrity verification supports supply chain assurance, tamper detection, and confidence that firmware and software protections are enforced on trusted platforms.

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: Developer security testing and evaluation ensures that security controls built into CCTV hardware, firmware, and software function as intended and do not introduce regressions over time. Testing activities address the full CCTV technology stack, including embedded firmware, operating systems, video processing libraries, management interfaces, cryptographic modules, network services, and interfaces to external systems such as VMS or storage platforms.

Security testing is integrated into the development lifecycle and performed whenever meaningful changes are introduced. This includes functional testing of security features, regression testing to ensure previously remediated issues do not reappear, and focused security testing of components that handle authentication, cryptographic operations, configuration management, or network exposure. Testing approaches are selected based on component criticality and operational risk, recognizing that not all CCTV components present the same attack surface.

Security testing results are documented, tracked, and resolved prior to release. Identified weaknesses are either remediated or formally dispositioned in accordance with the manufacturer’s

secure development and risk management processes. This control supports consistent security quality across firmware releases and reduces the likelihood that security weaknesses are introduced into field-deployed CCTV systems.

Parameter Value(s):

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

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

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

Risk References and Resources:

ARC-IT Mechanisms:

- Developers should conduct application security penetration testing before any major release.
- Testers should develop a test plan, execute it, and report on findings.
- All flaws identified must be properly documented and either remediated or accepted.

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

Responsible Party (M/I): M/I

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

Guidance: Threat modeling and vulnerability analysis are conducted as part of the CCTV secure development process to identify security risks before deployment. Analyses consider the CCTV operational environment, system architecture, data flows, trust boundaries, and anticipated adversary behaviors relevant to transportation and roadside deployments. Both system-level threats and component-specific vulnerabilities are evaluated, with particular emphasis on components that affect authentication, cryptographic protection, firmware update mechanisms, and data integrity.

Threat modeling activities inform design decisions and guide security testing priorities. Vulnerability analysis techniques include architectural review, code analysis, dependency analysis, and validation against known attack techniques. Findings are documented and reviewed by qualified security personnel, and identified high-severity vulnerabilities are resolved or formally accepted prior to release.

Parameter Value(s):

paragraph a. "FIPS 199 categorization, operational environment, known/assumed threats from MITRE ATT&CK, and acceptable risk defined by the IOO's risk management strategy"

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

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

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

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

Responsible Party (M/I): M/I

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

Guidance: Attack surface reviews identify and control externally reachable interfaces and services exposed by CCTV components. Reviews examine network ports, protocols, APIs, management interfaces, update mechanisms, debug features, and third-party dependencies that may increase exposure. This includes interfaces intended for maintenance, diagnostics, or integration with external systems.

Attack surface reviews verify that only required functionality is enabled, unused services are disabled, and security controls such as authentication, authorization, and input validation are consistently applied. Results are documented and maintained as part of the development of security record and updated whenever new interfaces, services, or dependencies are introduced.

SA-17, Developer Security and Privacy Architecture and Design

Responsible Party (M/I): M/I

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

Guidance

The manufacturer defines and documents the security and privacy architecture for the CCTV system as part of system design. The architecture describes trust boundaries, data flows, cryptographic protections, privilege separation, and secure communication paths between cameras, management interfaces, storage components, and external systems such as VMS or TMC platforms.

Security design incorporates layered protections, least privilege, secure defaults, authenticated update paths, and isolation of security-critical functions (e.g., credential storage, cryptographic operations, firmware verification). Privacy protections are embedded in data-handling functions, including minimization of collected data, configurable retention, controlled access to recordings, and support for masking or redaction where applicable.

Security and privacy architecture artifacts are maintained under configuration management and reviewed at defined design milestones to ensure that subsequent changes do not weaken established protections.

SA-22, Unsupported System Components

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: Unsupported CCTV components introduce unmitigated security and reliability risks. The organization identifies CCTV hardware, firmware, software, and storage components that are no longer supported by the manufacturer and evaluates their impact on confidentiality, integrity, availability, and roadway operations.

When components reach the end of support, they are replaced, upgraded, isolated, or mitigated through compensating controls based on risk. End-of-support timelines, known vulnerabilities, and available upgrade paths are tracked to prevent continued reliance on obsolete components. Where replacement is not immediately feasible, additional controls such as network segmentation, access restrictions, or enhanced monitoring are applied.

Parameter Value(s):

paragraph b. "organization-provided support or support from organization-approved external providers"

Risk References and Resources:

NIST SP 800-82⁽⁴⁾: 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 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:

CCTV systems separate system management functionality from operational user functionality to prevent non-privileged users from accessing security- or configuration-critical capabilities. Administrative functions such as firmware management, configuration changes, credential management, cryptographic configuration, and audit control are accessible only to privileged administrative roles.

Operational user functionality is limited to approved camera operations such as viewing live or recorded video, PTZ control within assigned permissions, and acknowledgment of system alerts. These functions are exposed through interfaces that do not permit access to operating system services, management shells, or security configuration.

Development and diagnostic functionality, where present, is isolated from both operational and administrative interfaces and is not accessible during normal system operation.

Risk References and Resources:

NIST SP 800-82: 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 of compensating controls include providing increased auditing measures.

ARC-IT Mechanisms:

- The device shall separate system management functionality from user application functionality by implementing all of the following:
 - The device requires an authentication mechanism for system management that is not used for any other function.
 - The device requires system management functions use memory that is either:
 - Dedicated exclusively to system management functions, or
 - Allocated dynamically to system management functions and not shared with non-management functions once allocated.

See also SC-39.

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: Non-privileged users access CCTV functionality through dedicated operator interfaces that exclude administrative or system-level capabilities. These interfaces support monitoring and operational tasks only and prevent access to configuration settings, firmware management, credential management, audit controls, or data deletion.

Functions with security or legal impact such as deleting recordings, exporting footage, modifying retention policies, or changing access permissions are restricted to privileged roles and are not exposed through non-privileged interfaces.

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: Security functions within the CCTV system are isolated from operational and user-facing functionality to prevent compromise of security controls through exploitation of video processing or user interfaces. Security functions include authentication, authorization enforcement, cryptographic operations, secure communications, audit generation, firmware verification, and integrity checking.

These functions execute in isolated execution contexts, such as separate processes, containers, or trusted execution environments, and do not share memory or execution privileges with non-security functions. Failure or compromise of operational components does not permit access to security-critical functions.

Risk References and Resources:

NIST SP 800-82⁽⁴⁾: Organizations consider implementing this control when designing new architectures or updating existing components. An example of 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.

NIST SP 800-82⁽⁴⁾: Personnel knowledgeable in security and privacy requirements are included in the change management process for the developer.

SC-3(1), Separation of System and User Functionality | Hardware Separation

Responsible Party (M/I): M

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

Guidance: For CCTV components that combine video processing and system management on the same device, hardware-based separation mechanisms are used to isolate security-critical functions from operational processing. Security functions such as cryptographic key handling, authentication, secure boot, and configuration integrity operate in processor modes, cores, or hardware security elements that are inaccessible to user-level or video-processing components.

This separation prevents compromise of video pipelines, codecs, or network interfaces from being leveraged to gain privileged or administrative access.

SC-3(2), Separation of System and User Functionality | Access and Flow Control Functions

Responsible Party (M/I): M

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

Guidance: Access control, information flow control, and audit functions are implemented in a manner that prevents bypass by operational software. These functions enforce authentication, authorization, and logging decisions independently of user-facing or video-processing components.

Where implemented in software, these functions operate in isolated execution contexts with restricted privileges. Where supported, hardware-assisted mechanisms are used to strengthen enforcement and reduce the risk of tampering or circumvention.

SC-3(3), Separation of System and User Functionality | 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 CCTV system minimizes non-security functionality within security-relevant components to reduce attack surface. Security components perform only those functions necessary to enforce authentication, authorization, cryptographic protection, integrity verification, and auditing.

Non-essential services, interfaces, and processing capabilities are excluded from security execution environments to prevent unintended interactions or exploitation paths.

SC-4, Information In Shared Resources

Responsible Party (M/I): M

Justification to Select: Threat "Obtain sensitive information via exfiltration" in table 3, Achieve Results (i.e., cause adverse impacts, obtain information).

Guidance: CCTV systems prevent unintended information disclosure through shared system resources such as memory, storage, temporary files, and processing buffers. Video data, metadata, and management information are isolated so that processes handling video capture, storage, analytics, and management do not inadvertently expose sensitive information to other processes or users.

Shared resources used by video management functions (e.g., NVR/DVR processes, export services, playback buffers) are cleared or reinitialized when released, and access to shared memory, temporary storage, and caches is restricted to authorized processes only. Where network-attached or centralized storage is used, logical separation is enforced between video data, system logs, and other organizational data to limit lateral exposure in the event of compromise.

Risk References and Resources:

NIST SP 800-82: This control is especially relevant for ITS systems that process confidential data. Example of compensating controls include engineering using the ITS to prevent sharing system resources.

ARC- IT Mechanisms:

- When a process, application, or user is finished using a sensitive shared resource, the resource shall be released in a way that all registers, memory, and temporary disk drives are properly erased/cleaned up so as not to leave any trace of the data.
- When a process, application, or user is using a sensitive shared resource, the users' process shall restrict access to any temporary system resources it is using to view the file (registers, memory, local disks).

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:

CCTV systems are protected against denial-of-service conditions that could disrupt video capture, transmission, storage, or management of functions. DoS protections address both malicious activity and operational stress conditions common in transportation environments, including excessive connection attempts, malformed network traffic, streaming overload, storage write saturation, and upstream network congestion.

DoS protections prioritize safety-critical functions, such as live video availability and camera health reporting, over non-essential services. When resource limits are reached, the system degrades in a

controlled manner (e.g., reduced frame rate) rather than failing unpredictably or becoming unavailable.

Network-facing interfaces, particularly management, API, and maintenance interfaces, enforce connection limits and rate controls to prevent resource exhaustion. Where applicable, upstream network devices (e.g., field switches, firewalls, or TMC routers) provide additional enforcement to protect constrained field devices.

Parameter Value(s):

paragraph a. #1 "Limit" #2 "network congestion, excessive stream requests, management interface flooding, storage write saturation, and power instability conditions"

paragraph b. "rate limiting on management and API interfaces; prioritization of live video and camera health telemetry; connection/session limits; protection against malformed traffic; controlled degradation of non-essential services; and stateful firewalling with connection tracking"

Risk References and Resources:

NIST SP 800-82⁽⁴⁾: 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.

ARC-IT Mechanisms:

- The application shall take the current environment into consideration when determining whether to verify, forward, or react to an incoming application datagram and shall not verify, forward or react to a datagram if it seems likely that this would lead to resource exhaustion.
- The application shall take the current environment into consideration when determining whether to cryptographically verify incoming application datagrams.
- The device shall discard IP packets whose source address is unknown to the device.
- The device shall discard IP packets whose source address is known to the device if the device does not have either:
 - A request pending to the source or
 - The source is on a whitelist of sources that may send the device to unsolicited IP traffic.
- The device shall enforce a limit on transmission of data over DSRC media.
 - This limit shall be configurable through a system management function.
 - This limit shall be:
 - no higher than 0.6 megabits per second on the DSRC safety channel (rationale: a single device shall not be able to use more than 10% of channel capacity of the safety channel) .
 - no higher than 1.2 megabit per second on 10 MHz DSRC service channels, and no higher than 2.4 megabits per second on 20 MHz service channels (rationale: a single device shall not be able to use more than 20% of channel capacity on service channels).

NOTE: The above limits represent maximums. Future versions of this document may include dynamic controls on these limits so that they go down if channel utilization is high.

- The device shall support notifying applications if the Channel Busy Ratio on channels used by those applications is greater than a configurable threshold.

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:

CCTV components are configured to prevent their use as platforms for launching denial-of-service or traffic amplification attacks against other systems. Outbound network behavior is constrained so that cameras, NVRs, and associated devices generate only expected traffic patterns to authorized destinations.

Network segmentation and traffic filtering prevent CCTV devices from originating broadcast, reflection, or high-volume unsolicited traffic that could impact other ITS field devices, controllers, or enterprise systems.

Parameter Value(s): “UDP flooding, ICMP amplification, broadcast traffic abuse”

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:

CCTV components are provisioned with sufficient processing capacity, memory, storage throughput, and network bandwidth to support expected peak operational loads, including simultaneous live viewing, recording, and health monitoring.

Network interfaces and upstream infrastructure are sized to tolerate transient traffic spikes without disrupting video streams. Where redundancy is feasible, buffering, queue management, or alternate network paths are used to reduce the likelihood that localized overload conditions result in complete loss of service.

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:

CCTV systems monitor indicators of denial-of-service conditions affecting cameras, storage, or network connectivity. Monitoring detects abnormal traffic rates, repeated connection failures, stream

interruptions, storage write failures, and resource exhaustion events that could indicate active attacks or emerging operational issues.

Alerts are generated when defined thresholds are exceeded or when critical services degrade, enabling timely investigation and mitigation before loss of situational awareness occurs.

Parameter Value(s):

paragraph a. “camera health polling, stream availability monitoring, bandwidth utilization thresholds, storage capacity alarms, and correlation with centralized monitoring or SIEM platforms for stream or device failures”

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:

CCTV systems are designed to maintain the availability of essential resources required for continuous video capture, encoding, transmission, and health monitoring under normal and peak operating conditions. Core resources include processor capacity, memory, storage of I/O, and network bandwidth at the camera, intermediate network devices, and any attached recording or management components.

Resource allocation prioritizes safety-critical and operationally essential functions, such as live video streams, camera status reporting, and fault detection, over non-essential services such as historical playback or diagnostics. When resources become constrained, the system degrades gracefully (e.g., reduced frame rate, adaptive bitrate, deferred non-critical processing) rather than dropping streams or becoming unresponsive.

SC-7, Boundary Protection

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.

CCTVs are becoming more advanced and, therefore, often provide connectivity beyond that to/from the TMC. As such, it is necessary to provide boundary protection to ensure only authorized communications are used to perform approved functions. It is not advisable to rely solely on routers external to the CCTVs, such as at the TMC, regional network boundaries, or other ITS shelter locations, as there may be other connections to the CCTVs that need to be managed.

Guidance:

CCTV systems in transportation environments operate at the edge of the network and often communicate with multiple backend components, including Traffic Management Centers (TMCs), video management systems, and storage platforms. Boundary protection is required to ensure that only authorized communications necessary for approved operational functions are permitted.

Boundary enforcement is implemented as close to the CCTV device as practical and does not rely solely on centralized protections at the TMC or enterprise perimeter. Each CCTV component enforces logical communication boundaries that restrict inbound and outbound traffic based on defined peers, protocols, and functions. Publicly accessible networks are not used for direct CCTV communications.

Boundary protection mechanisms limit exposure from unauthorized hosts, prevent lateral movement between field devices, and ensure that management, update, and diagnostic interfaces are accessible only through controlled paths.

Parameter Value(s):

paragraph b. "logically"

Risk and Resources:

ATT&CK for ICS Mitigations / Techniques:

- M0935 / T0822
- M0937 / T0806, T0868, T0816, T0839, T0861, T0843, T0845, T0886, T0856, T0857, T0855, T0859

ARC-IT Mechanisms:

- The device shall maintain a mechanism for monitoring all communications that cross its boundary, such that:
 - All communications can be scanned and optionally logged irrespective of the function those communications are associated with:
 - Communications monitoring diagnostics and settings are restricted from general application use.
 - Communications monitoring diagnostics and settings may be modified through an administrative interface.
- The device shall discard IP packets whose source address is known to the device if the device does not have either:
 - A request pending to the source.
 - The source is on a whitelist of sources that may send the device to unsolicited IP traffic.
- The device shall discard IP packets whose source address is unknown to the device.
- The device shall monitor the status of its inbound firewall. If its firewall is not operating, the device:
 - Shall not accept any data from external sources targeting management, security, or application update functions (Fail Secure)
- The device shall provide support for assigning applications to categories such that two applications may only exchange data if they are classified in the same category. The device may support assigning one application to more than one category. The device shall support at least four application categories and may support more.

SC-7(3), Boundary Protection | Access Points

Responsible Party (M/I): I

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

Guidance: Access points represent controlled interfaces where external entities may connect into the ITS network that supports CCTV operations. These access points are limited in number, explicitly authorized, and documented. External connectivity such as remote maintenance or diagnostics is permitted only through managed access points and not directly to roadside CCTV devices.

Risk References:

ARC-IT Mechanisms: See SC-7.

SC-7(5), Boundary Protection | Deny by Default — Allow by Exception

Responsible Party (M/I): I

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

Guidance: CCTV communication peers are known in advance and limited to specific systems such as the TMC, authorized video management servers, and approved storage platforms. Boundary enforcement uses an allow-list approach in which only explicitly authorized devices, protocols, and services are permitted. All other communications are blocked by default.

Parameter Value(s):

"at managed interfaces; for all IP cameras, video encoders, PTZ actuators, and VMS servers"

Risk References:

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: Remote devices used for CCTV administration or maintenance are prohibited from split tunneling while connected to the ITS network. Remote access sessions route all traffic through approved secure tunnels to prevent exposure to untrusted networks during privileged operations.

Parameter Value(s):

"Mandated VPN use"

SC-7(14), Boundary Protection | Protect Against Unauthorized Physical Connections

Responsible Party (M/I): M/I

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

Guidance: CCTV devices are deployed in publicly accessible roadside environments where physical access cannot be fully prevented. Communication boundaries are reinforced through physical controls that limit unauthorized connection to network and device interfaces. These controls include locked enclosures, protected cabling, tamper-resistant connectors, and controlled access to exposed ports.

Parameter Value(s):

“Video ports, External device ports”

Standards: IEEE 802.1X⁽⁴⁰⁾ & 802.3⁽⁴¹⁾

SC-7(15), Boundary Protection | Networked Privileged Accesses

Responsible Party (M/I): M/I

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

Guidance: Privileged network access for configuration, diagnostics, and updates is restricted to dedicated management paths that are logically separated from operational video traffic. Privileged sessions traverse managed interfaces that enforce authentication, authorization, and logging and are not permitted over general-purpose data paths.

SC-7(16), Boundary Protection | Prevent Discovery of System Components

Responsible Party (M/I): M

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

Guidance: CCTV devices limit their response to network discovery, scanning, and enumeration attempts. Management and backend system addresses are not disclosed through unauthenticated queries, broadcast responses, or error messages.

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: CCTV systems only accept communications from organizationally approved hosts and devices. Communications from unknown or unconfigured sources are blocked prior to authentication.

Parameter Value(s):

“Individual IP cameras, analog cameras, physically or wireless attached video management systems or storage devices.”

SC-7(20), Boundary Protection | Dynamic Isolation and Segregation

Responsible Party (M/I): M/I

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

Guidance:

CCTV components support isolation when abnormal behavior, suspected compromise, or operational risk is detected. Isolation mechanisms prevent affected components from interacting with other ITS systems while preserving basic safety visibility where feasible. Isolation may be achieved through network segmentation, VLAN reassignment, or policy-based traffic blocking.

Parameter Value(s):

"IP cameras, video encoders, and edge storage units"

Risk References:

NTCIP1205

SC-7(21), Boundary Protection | Isolation of System Components

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.

Guidance: CCTV components are logically separated from other field devices through VLANs or equivalent segmentation to reduce the impact of compromise and prevent lateral movement between ITS subsystems.

Parameter Value(s):

#1. "IP cameras, video encoders, and edge storage units"

Risk References:

ARC-IT Mechanisms: See SC-07.

SC-7(24), Boundary Protection | Personally Identifiable Information

Responsible Party (M/I): M/I

Justification to Select: Threat "Obtain sensitive information via exfiltration" in table 3, Achieve Results (i.e., cause adverse impacts, obtain information).

Guidance: CCTV systems deployed in public spaces may capture PII such as faces or license plates. It is essential that the processing, storage, and transmission of such information adhere to applicable laws and internal organizational privacy policies. The IOO is responsible for establishing the privacy requirements for PII captured by CCTV and clearly communicates privacy requirements to the manufacturer/vendor to guide system design and configuration. Privacy protections may include redaction features (e.g., blurring), access controls, and secure transmission protocols.

Parameter Value(s):

- " Encrypt data at rest using organizationally approved algorithms",
- " Enforce organizational retention and disposal policies",
- " Apply anonymization or redaction where required"

Standards: NIST SP 800-122⁽³⁶⁾

SC-7(28), Boundary Protection | External Connections

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: Direct connections between CCTV systems and public networks are not permitted. External entities, including vendors, access CCTV systems only through approved organizational access points within the managed ITS network.

Parameter Value(s):

"All systems"

Risk References:

NIST SP 800-82⁽⁴⁾: 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 "Conduct externally based network traffic modification (man in the middle) attacks" in table 3, Conduct an Attack (i.e., direct/coordinate attack tools or activities).

Threat "Conduct internally-based network traffic modification (man in the middle) attacks" in table 3 Conduct an Attack (i.e., direct/coordinate attack tools or activities).

Threat event "Perform network sniffing of exposed networks" in table 3, Perform Reconnaissance and Gather Information.

The control applies to components that transmit or receive information, as communication paths outside the physical protection of a controlled boundary are exposed to the possibility of interception and modification.

Guidance: CCTV devices protect the confidentiality and integrity of video streams, control commands (including PTZ), and management of traffic transmitted over networks. Protections apply to communications between cameras, encoders, storage systems, VMS components, and the Traffic Management Center.

Transmission protections are implemented using standardized cryptographic protocols that provide peer authentication and message integrity, and where required, confidentiality. Protocols and cipher suites are selected from organization-approved standards and configured to prevent unauthorized interception, modification, replay, or injection of traffic.

Unencrypted or unauthenticated network services used for video streaming, device management, or control are disabled unless explicitly required for operational reasons and approved through documented risk acceptance. Where encryption cannot be applied due to operational or performance constraints, integrity protection and authenticated peer verification are enforced to prevent command or data manipulation.

Parameter Value(s):

“Confidentiality and integrity of video and control traffic by preventing unauthorized disclosure and detecting any modification or spoofing attempts.”

Risk References:

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

ARC-IT Mechanisms:

- Role-based access control as specified in the Access Control family with cryptographically enforced integrity checking:
 - VPN or SSL with 128-bit security symmetric cryptography for two-way information flows using strong password or X.509 certificates for integrity protection
 - VPN or SSL with 128-bit security symmetric cryptography for two-way information flows using strong password or X.509 certificates for confidentiality protection
 - IEEE 1609.2 authentication for incoming information flows

Standards: RFC 8446⁽¹⁴⁾.

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: CCTV devices use cryptographic mechanisms to protect information transmitted across network segments that are not physically protected or otherwise trusted. Cryptographic protections ensure that video, metadata, and control traffic are authenticated and protected against modification, and where required, encrypted to prevent unauthorized disclosure.

Cryptographic modules and algorithms are selected in accordance with organizational policy and applicable standards, including FIPS 140-3 where feasible. Authenticated encryption modes or equivalent integrity-protecting mechanisms are used to ensure that transmitted data cannot be altered without detection.

Device and service authentication is performed prior to data exchange using certificate-based or equivalent cryptographic credentials. Failures in cryptographic verification or authentication are detected and logged for security monitoring.

Parameter Value(s):

“Cryptographic mechanisms are used to protect the confidentiality and integrity of video, control, and management traffic transmitted over untrusted or shared networks.”

Risk References:

NIST SP 800-82⁽⁴⁾: 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.

Standards: FIPS 140-3⁽¹⁸⁾

SC-10, Network Disconnect

Responsible Party (M/I): M

Justification to Select: Threat "Denial of Control" in table 5.

The control applies to typical and atypical information technology that transmits or receives information. Communication paths that remain established beyond their usefulness unnecessarily expose transmitted information to the possibility of interception. Physical objects within the scope of this control set transmit or receive information; therefore, the control applies and is implemented on the physical object or possibly the distant end, either in a typical manner if resources permit or in an atypical manner to provide equivalent protections.

Guidance: This control applies to interactive or on-demand network sessions established for local or remote user access to CCTV components, such as configuration, diagnostics, maintenance, or application development activities. These sessions are terminated after a defined period of inactivity to reduce the exposure of management and control interfaces.

CCTV devices automatically disconnect inactive user-initiated sessions (e.g., local console access, maintenance of laptop connections, administrative web interfaces, or API configuration sessions) after the organization-defined timeout period. Timeouts are selected based on the sensitivity of the functions performed and the risk of unauthorized access in the deployment environment.

Parameter Value(s):

“No more than 10 minutes of inactivity for user-initiated network or local management sessions.”

Risk References:

ARC-IT Mechanisms:

- For TCP/IP ports in any state other than “LISTENING,” the device should de-allocate that TCP/IP port once 15 minutes have passed with no activity on that port.
- For User Datagram Protocol (UDP)/IP ports in any state other than “LISTENING,” the device should de-allocate that UDP/IP port once 15 minutes have passed with no activity on that port.

ARC-IT Mechanisms: See SC-8.

SC-11, Trusted Path

Responsible Party (M/I): M

Justification to Select: Threat events “Perform network sniffing of exposed networks” in table 3, Perform Reconnaissance and Gather Information, and “Obtain sensitive information through network sniffing of external networks” in table 3, Achieve Results (i.e., cause adverse impacts, obtain information).

Guidance: CCTV systems must provide a trusted communication path for accessing security-critical functions such as authentication, authorization management, cryptographic configuration, firmware management, and security logging. The trusted path ensures that credentials, commands, and responses exchanged between the user and the CCTV are protected from interception, modification, or redirection by untrusted processes, network segments, or intermediary systems.

In a transportation CCTV deployment, the trusted path is typically implemented as a logically isolated management channel that is separate from video streaming and general operational traffic. This path uses authenticated, encrypted protocols and terminates directly at the CCTV security or management interface, preventing exposure through shared services, application interfaces, or non-secure network paths.

Trusted paths apply to both local access (e.g., maintenance laptop connected to the field cabinet) and remote access (e.g., administrative access from the TMC) and are enforced whenever privileged users interact with security-relevant system functions. User interfaces and APIs that do not provide trusted-path protections are prohibited from performing security-sensitive operations.

Parameter Value(s):

paragraph b. “security and management functions, including authentication, access control configuration, cryptographic settings, firmware updates, and audit configuration”

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: CCTV devices must employ cryptographic protections to preserve the confidentiality, integrity, and authenticity of video, control, management, and audit data during transmission and storage when such data traverses untrusted networks or resides on shared or removable media.

Cryptographic mechanisms must be implemented using modules validated under FIPS 140-3 and configured in accordance with organizational cryptographic policy. For IP-based communications, CCTV devices support industry-standard, well-vetted secure communication protocols (e.g., TLS) with authenticated endpoints to protect against interception, spoofing, and unauthorized modification of data. Mutual authentication is required where CCTV devices exchange management, control, or configuration data with trusted external systems such as the TMC, VMS, or centralized storage.

Cryptographic keys, credentials, and trust anchors are generated, stored, and used in a manner that prevents unauthorized disclosure or extraction. Where supported by the platform, private keys are protected using hardware-backed mechanisms (e.g., secure elements or trusted execution environments). Cryptographic operations rely on approved deterministic random bit generators consistent with NIST guidance.

Certificate provisioning, rotation, and revocation are performed in a controlled manner to maintain trust relationships throughout the operational lifecycle of the CCTV system, including commissioning, maintenance, and decommissioning.

Risk References:

ARC-IT Mechanisms:

- Devices may support additional cryptographic algorithms.
- Devices should provide a random number generator compliant with FIPS 140-2⁽¹⁶⁾ (i.e., compliant with NIST SP 800-90A rev 1⁽²²⁾).

Standards: FIPS 140-3⁽¹⁸⁾

SC-16, Transmission of Security and Privacy Attributes

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: When CCTV data is transmitted to external systems such as the TMC, VMS, or centralized storage, associated security and privacy attributes are preserved and protected against loss, alteration, or mis binding. This ensures that access control decisions, audit records, and privacy safeguards applied at the source remain effective after transmission and ingestion by receiving systems.

Transmission of these attributes occurs over authenticated and integrity-protected communication paths, and attributes are bound to the associated video streams, control messages, or audit records in a manner that prevents spoofing or stripping. Attribute handling supports operational use cases common to transportation systems, including incident response, evidentiary review, interagency sharing, and privacy-aware disclosure.

Parameter Value(s): "User role and privilege context, access control decisions, audit and event correlation identifiers, data sensitivity or privacy indicators"

SC-17, Public Key Infrastructure Certificates

Responsible Party (M/I): M/I

Justification to Select: Threat event “Craft counterfeit certificates” in table 3, Craft or Create Attack Tools.

Guidance: CCTV devices rely on public key certificates to establish trusted identities for devices, services, and management interfaces. Certificate-based trust enables authenticated communications, prevents device impersonation, and supports secure integration with transportation and enterprise systems.

CCTV systems should support multiple certificate trust models, allowing the IOO to select the approach that best aligns with operational architecture and risk tolerance. At a minimum, devices support X.509-based public key infrastructure for secure management and administrative access. Where CCTV systems participate in connected transportation environments or edge-based ITS communications, devices may also support IEEE 1609.2 certificates issued through a Security Credential Management System (SCMS).

When SCMS credentials are used, CCTV devices support enrollment and operation consistent with IEEE 1609.2, including the use of application identifiers such as Provider Service Identifiers (PSIDs) and associated Service Specific Permissions (SSPs) to constrain the purpose and scope of device communications (e.g., video streaming, status reporting, or event notification). This enables fine-grained authorization at the edge and limits misuse of device credentials beyond approved ITS functions.

X.509 certificates may be used in parallel or independently to support remote system management, administrative access, and integration with enterprise security infrastructure, including identity-based access control and centralized monitoring systems. This allows separation between operational device trust and user or administrator identity management when appropriate.

CCTV devices support secure certificate enrollment and lifecycle management, which may occur during manufacturing, field commissioning, or initial connection to the TMC or another IOO-managed system. Enrollment mechanisms ensure device authenticity prior to certificate issuance and may include pre-provisioned credentials, authenticated enrollment protocols, or controlled local commissioning procedures. Certificate renewal and revocation processes are designed to accommodate field-deployed devices with intermittent connectivity.

Parameter Value(s):

paragraph a. "X.509 public key certificates issued by an IOO-approved or enterprise certificate authority; IEEE 1609.2 certificates issued via an approved SCMS, including PSID and SSP constraints for authorized CCTV applications"

SC-23, Session Authenticity

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:

For IP-based communications, CCTV devices establish session authenticity using mutually authenticated secure session protocols, such as TLS or IPsec, that bind session state to authenticated device or service identities. Session establishment includes verification of peer credentials and cryptographic negotiation that prevents downgrade, replay, or man-in-the-middle attacks.

Where CCTV devices participate in connected transportation or edge-based ITS environments using IEEE 1609.2 certificates, session authenticity may also be established using ISO/IEC 21177-compliant secure session mechanisms. In such cases, authenticated session establishment leverages certificate-based trust and application context (e.g., PSID/SSP) to ensure sessions are bound to authorized purposes and endpoints.

Any additional session-oriented protocols used for administration or maintenance (e.g., secure remote access or command interfaces) employ equivalent protections to ensure session authenticity and prevent reuse or interception of session identifiers. Session parameters and cryptographic mechanisms are selected from currently approved standards and reviewed over time as algorithms and protocol guidance evolves.

Risk References:

ATT&CK for ICS Mitigations / Techniques:

- M0802 / T0830, T0858, T0868, T0816, T0831, T0832, T0839, T0843, T0845, T0856, T0857, T0855

NIST SP 800-82⁽⁴⁾: Example compensating controls include auditing measures.

ARC-IT Mechanisms:

- Approved mechanisms for session authenticity are TLS and Internet Protocol Security (IPSec) with the following parameters, which must be periodically reviewed as algorithms age over time and key size recommendations are updated:
 - TLS 1.2⁽²⁰⁾ or preferably 1.3⁽¹⁴⁾ using algorithms currently approved by NIST, with key sizes appropriate for this use.
 - IPSec using algorithms based on the Advanced Encryption Standard⁽²⁴⁾ currently approved by NIST.
- The device should support at least one of these mechanisms.

Standards: ISO 21177, RFC 8446⁽¹⁴⁾

SC-23(1), Session Authenticity | Invalidate Session Identifiers at Logout

Responsible Party (M/I): M

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

Guidance: Upon user logout, all session material should be deleted at the CCTV, including session identifiers and any derived cryptographic material.

SC-28, Protection of Information at Rest

Responsible Party (M/I): M

Justification to Select: Encryption of information in storage (i.e., data-at-rest) protects the confidentiality and integrity of the information.

Guidance: Upon user logout, session timeout, or termination of a management or maintenance connection, the CCTV device must invalidate and remove all session-related states. This includes session identifiers, authentication tokens, cached credentials, and any session-specific cryptographic material. Session invalidation prevents reuse of stale sessions and reduces the risk of session hijacking, replay, or unauthorized continuation of privileged access.

Parameter Value(s):

- #1 "Confidentiality & Integrity",
- #2 "Surveillance footage"

Risk References:

ATT&CK for ICS Mitigations / Techniques:

- M0941 / T0839, T0857

NIST SP 800-82⁽⁴⁾: The use of cryptographic mechanisms is implemented only after careful consideration and after verification that it does not adversely impact the operational performance of the ITS. Cryptographic mechanisms may not be feasible on certain ITS devices. In these cases, compensating controls may be relocating the data to a location that does support cryptographic mechanisms.

ARC-IT Mechanisms:

- The device should encrypt data on disk if that data is accessed only by entities with periodic privileged access as defined in Notes on Access Control.⁽¹³⁾
- The device may encrypt data on disk if that data is accessed by entities with ongoing privileged access or with no privileges.
- Keys used to encrypt data on disk should be protected by hardware of at least FIPS 140-2⁽¹⁶⁾ level 2-equivalent security, such that they cannot be used other than by booting the device.

SC-28(1), Protection of Information at Rest | Cryptographic Protection

Responsible Party: M

Justification to Select: Encryption of information in storage (i.e., data-at-rest) protects the confidentiality and integrity of the information.

Guidance: This technical control applies to all information stored by CCTV components, including video footage, associated metadata, configuration data, audit logs, and system files stored on cameras, DVRs, NVRs, and attached or remote storage systems. Stored video and metadata must be protected using strong cryptographic mechanisms implemented in FIPS 140-3-validated cryptographic modules.

Encryption is applied at the storage layer (e.g., full-disk, volume, or file-level encryption) using approved algorithms such as AES with key lengths appropriate for the sensitivity of the data. Integrity protection mechanisms ensure stored content cannot be modified without detection prior to playback, export, or transfer. Backup copies of CCTV data must receive equivalent cryptographic protection prior to offload or transport.

Parameter Value(s):

#1 “all system components and media”

#2 “all information”

SC-28(3), Protection of Information at Rest | Cryptographic Keys

Responsible Party: M

Justification to Select: Encryption of information in storage (i.e., data-at-rest) protects the confidentiality and integrity of the information.

Guidance: Cryptographic keys used to protect information at rest must be stored and used in a protected manner to prevent unauthorized disclosure or misuse. CCTV devices should employ hardware-backed key protection mechanisms that were supported by the platform, particularly for roadside or unattended deployments.

Key storage mechanisms are selected to align with the deployment environment and risk profile and may include trusted execution environments, secure elements, or hardware security modules integrated into the device. Software-only key storage is permitted only where hardware protection is not feasible and compensating controls are applied.

Parameter Value(s):

“FIPS 140-3 validated cryptographic module, Trusted Platform Module, HSM or secure element (SE)”

Standards: ISO / ISE 11889:2015(TPM)⁽⁴²⁾, TPM 2.0 library specification, ISO / ISC 19790⁽⁴³⁾, FIPS 140-3⁽¹⁸⁾, NIST SP 800-57 part 1⁽⁴²⁾, NIST SP 800-111⁽³³⁾

SC-32, System Partitioning

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: CCTV systems must be partitioned to limit the impact of compromise, misconfiguration, or failure of individual components. Partitioning separates critical functions such as camera control, video processing, storage, management, and external communications so that a fault or attack in one function does not propagate to others.

In typical transportation deployments, partitioning is achieved through a combination of logical separation (e.g., distinct processes, containers, virtual machines, or OS privilege domains) and physical separation (e.g., discrete cameras, NVRs, storage appliances, and management systems). Management and administrative functions are isolated from operational video streams, and security-relevant services are not co-resident with user-accessible or externally exposed services.

Parameter Value(s):

#1 "video capture and control, video processing, storage, management, and external communications"

#2 "physical and logical"

#3 "security categorization and operational criticality"

Risk References:

NIST SP 800-82: Organizations consider separate physical domains for privileged functions, such as those that affect security and safety

SC-35, External Malicious Code Identification

Responsible Party (M/I): M

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

Guidance: CCTV systems must include mechanisms to detect and prevent the introduction of malicious code through external interfaces such as network connections, removable media, maintenance ports, or software update mechanisms. Controls focus on prevention rather than traditional endpoint malware scanning, which is often impractical for embedded and real-time systems.

Malicious code protection is implemented through allowlisting of executable code, cryptographic verification of firmware and software updates, restricted execution environments, and disabling of unused services and interfaces. Where applicable, integrity monitoring detects unauthorized changes to system binaries or configuration files. These mechanisms ensure that only authorized and validated software is executed on the CCTV device.

SC-36, Distributed Processing and Storage

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: Where required to support availability, scalability, or resilience, CCTV processing and storage functions may be distributed across multiple physical locations or logical domains. This includes separating cameras from video recorders, distributing storage across multiple devices, or leveraging redundant processing nodes.

Distributed designs ensure that the loss, degradation, or compromise of a single device does not result in loss of all video capability for a corridor or region. Data replication and failover mechanisms preserve video integrity and availability while maintaining secure communication paths between distributed components.

Parameter Value(s):

#1 "Physical and logical"

SC-39, Process Isolation

Responsible Party (M/I): M

Justification to Select: Vulnerability "Control network services dependent on a non-control network" in table 6, Architecture and Design Vulnerabilities and Predisposing Conditions.

Guidance: CCTV systems must isolate executing processes to prevent faults or compromises in one process from affecting others. Video capture, encoding, storage, management, security services, and update mechanisms operate in separate execution contexts with distinct memory spaces and privilege levels.

Security-critical functions such as authentication, cryptographic operations, and configuration management are isolated from video processing and user-facing functions. Isolation may be implemented using operating system protections, process sandboxing, containerization, or microkernel-based architectures appropriate to the device platform.

Risk References and Resources:

NIST SP 800-82⁽⁴⁾: Example compensating controls include partition processes to separate platforms.

ARC-IT Mechanisms:

- Devices should provide a separate address space for each executing process.
- Devices should ensure that access to protected resources, including signing keys, is only granted to processes that have the appropriate permissions per AC-3.
- Devices should provide address space layout randomization, data execution prevention, and application sandboxing.

SC-39(1), Process Isolation | Hardware Separation

Responsible Party (M/I): M

Justification to Select: Vulnerability "Control network services dependent on a non-control network" in table 6, Architecture and Design Vulnerabilities and Predisposing Conditions.

Guidance: For CCTV components that perform both operational and security-sensitive functions, hardware-based separation is used where it is feasible to strengthen isolation. This includes separating security-critical functions such as cryptographic processing, secure boot, or key storage, from general-purpose processing used for video handling and network communications.

Hardware separation may be implemented through dedicated security processors, trusted execution environments, or memory protection mechanisms that prevent user-accessible or externally influenced processes from interacting with protected functions.

SC-40, Wireless Link Protection

Responsible Party: 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: For Wi-Fi-based links, the CCTV system must enforce strong link-layer security using current, standards-based protections (e.g., WPA3-Enterprise or WPA2-Enterprise where WPA3 is not supported), with mutual authentication and encryption enabled. Open, pre-shared key, or consumer-grade security modes are not permitted. Wi-Fi interfaces are disabled by default unless operationally required.

For cellular connections, reliance on carrier-provided security alone is insufficient. CCTV systems must protect all application-layer traffic over cellular links using authenticated encryption (e.g., TLS or IPsec), ensuring confidentiality and integrity regardless of underlying network protections. Cellular interfaces are restricted to approved access points and management endpoints only.

Wireless interfaces are configured with least functionality principles, limiting exposed services, disabling ad hoc or peer-to-peer modes, and preventing unauthorized association. Monitoring and logging of wireless link status and security-relevant events support detection of anomalous behavior or degradation.

Parameter Value(s):

“802.11 a/b/g/n/ac/ax with enterprise security modes enabled; cellular LTE or 5G links protected with end-to-end encrypted application traffic”

Standards: NTCIP 1205⁽²⁹⁾

SC-41, Port and I/O Device Access

Responsible Party: 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: CCTV devices and associated storage components often include physical and logical ports that are not required for normal operation, such as maintenance, debugging, or factory test interfaces. If left enabled or accessible, these ports can provide a direct path for unauthorized access, bypassing network-based security controls.

CCTV systems must restrict access to ports and I/O interfaces to only those required for operational use, maintenance, or approved diagnostics. Unused physical ports are disabled, blocked, or physically protected prior to deployment. Where ports cannot be disabled in software, physical protections such as port blockers, sealed connectors, internal placement within locked housings, or removal of headers are used to prevent access.

Access to required ports is limited to authorized maintenance activities and protected through physical security controls, authenticated sessions, or both. Configuration changes affecting port availability are controlled and documented as part of system configuration management.

Parameter Value(s):

#1 "physically restrict or disable" #2 "all unused physical ports and I/O interfaces, including UART, USB, Ethernet, I2C, SPI, JTAG, and serial debug ports"

Risk References:

NIST SP 800-82⁽⁴⁾: 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: Usage restrictions define what functions CCTV components are permitted to perform during normal operation and under what conditions those functions may be exercised. In transportation of CCTV deployments, misuse of camera control, video transmission, or maintenance interfaces can directly affect operational awareness, incident response, and roadway safety.

CCTV systems enforce usage restrictions by limiting available functions based on roles, context, and operational state. Examples include restricting pan-tilt-zoom (PTZ) control to authorized operators, limiting configuration and firmware functions to maintenance windows, and preventing use of diagnostic or test functions during live operations. Only approved functions required for traffic monitoring, incident detection, and system health are enabled.

Parameter Value(s):

"Camera control interfaces (including PTZ), video transmission functions, and system or maintenance interfaces on cameras, camera controllers, and management processors"

Standards: NTCIP1205⁽²⁹⁾

SC-49, Hardware-Enforced Separation and Policy Enforcement

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: CCTV systems implement hardware-enforced separation using mechanisms such as processor privilege levels, hardware memory protection, trusted execution environments, or dedicated security processors. These mechanisms ensure that security-critical functions cannot be accessed or modified by non-security processes, even if application-level software is compromised.

Policy enforcement associated with hardware separation ensures that security boundaries remain intact during normal operation, maintenance, and updates, and that violations result in controlled failure or restricted functionality rather than unsafe operation.

Parameter Value(s): "Video capture and processing, cryptographic operations, access control enforcement, and remote management or maintenance functions"

SC-51, Hardware-Based Protection

Responsible Party (M/I): M

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

Guidance: Hardware-based protection mechanisms provide foundational safeguards for CCTV components deployed in publicly accessible or roadside environments. These mechanisms protect against both physical tampering and attempts to subvert to system of integrity through unauthorized modification.

CCTV systems incorporate hardware protections such as secure boot, immutable bootloaders, write-protected storage regions, and tamper-resistant or tamper-evident enclosures. These protections ensure that only authorized firmware and software can execute and that physical access does not directly translate into control of system behavior.

Parameter Value(s):

paragraph a. "Secure boot enforcement, write-protected system components, and tamper-resistant or tamper-evident hardware features"

paragraph b. "Local Device administrators"

Risk References:

NIST SP 800-82⁽⁴⁾: Some ITS systems support write-protection by implementing physical key switches or write-protect switches. Organizations define the systems for which write-protection will be enabled and develop a process for how to take the system out of write-protect mode.

SI Family – System and Information Integrity

SI-2, Flaw Remediation

Responsible Party: M/I

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

Guidance: The IOO establishes and enforces a flaw remediation process for CCTV systems that addresses identified vulnerabilities in hardware, firmware, and software components.

Manufacturers identify, analyze, and document security flaws affecting CCTV components and provide validated remediation artifacts, including firmware updates, software patches, configuration changes, or documented mitigations. Remediation artifacts include impact descriptions, affected versions, operational considerations, and installation constraints applicable to field-deployed devices.

The IOO evaluates manufacturer-provided remediation and determines deployment timing based on operational constraints. Where immediate remediation is not feasible, the IOO implements compensating controls, including service restriction, network isolation, access limitation, increased monitoring, or temporary configuration changes, until remediation can be applied.

When no remediation is available, manufacturers provide recommended mitigations or detection guidance to reduce exposure. Flaw remediation status, compensating controls, and risk acceptance decisions are tracked as part of the CCTV vulnerability management process.

Parameter Value(s):

paragraph c. "less than 30 days"

Risk References:

ATT&CK for ICS Mitigations / Techniques:

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

NIST SP 800-82⁽⁴⁾: 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's 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, and 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-3, Malicious Code Protection

Responsible Party: M/I

Justification to Select: Threat insert specialized malware into organizational information systems based on system configurations" in table 3, Deliver/Insert/Install Malicious Capabilities.

Vulnerability "Malware protection implemented without sufficient testing" in table 6, Policy and Procedure Vulnerabilities and Predisposing Conditions.

Guidance: Malicious code protection for CCTV systems is implemented in a manner that does not interfere with real-time video capture, control, or transmission functions.

Manufacturers design CCTV components to prevent the execution of unauthorized or untrusted code through mechanisms such as secure boot, signed firmware and software enforcement, and execution allowlisting. Where feasible, detection mechanisms are implemented to identify attempted execution or introduction of malicious code through network interfaces, maintenance ports, removable media, or update mechanisms.

The IOO determines where malicious code protection is applied based on system role and operational impact. For field-deployed cameras and edge devices, protection emphasizes prevention and detection rather than continuous active scanning. For centrally managed components (e.g., VMS servers, NVRs, management workstations), additional signature-based or behavior-based protections may be employed where they can be validated not to disrupt operations.

Parameter Value(s):

paragraph a. signature based

paragraph c.1 #1 "At least weekly."

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

paragraph c.2 #1 "Block and quarantine malicious code"

paragraph c.2 #2 "Security Admins, System Admins, and any other pertinent personnel or roles"

Risk References:

ATT&CK for ICS Mitigations / Techniques:

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

NIST SP 800-82⁽⁴⁾: 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 of 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

Justification to Select: Vulnerability "Malware protection implemented without sufficient testing" in able 6, Policy and Procedure Vulnerabilities and Predisposing Conditions.

Guidance: Updates to malicious code protection mechanisms, including signature databases, allowlists, detection rules, and enforcement policies, are restricted to privileged users only.

Manufacturers ensure that update mechanisms for malicious code protection require authenticated and authorized administrative access and that updates are integrity-protected. The IOO defines which roles are authorized to approve and deploy updates and ensures updates are tested or staged, as appropriate, prior to deployment on operational CCTV components.

Automated updates may be enabled only for components where such updates do not introduce operational risk. For field-deployed devices, update actions are controlled and logged to ensure traceability and rollback capability.

SI-4, System Monitoring

Responsible Party: M/I

Justification to Select: Threat "Install persistent and targeted sniffers on organizational information systems and networks" in table 3, Deliver/Insert/Install Malicious Capabilities.

Vulnerability "Intrusion detection and prevention software is not installed" in table 6, Policy and Procedure Vulnerabilities and Predisposing Conditions.

Guidance: Monitoring capabilities include device uptime, processor utilization, memory availability, storage capacity, camera status, stream availability, and interface health. Security-relevant events such as authentication failures, unauthorized configuration changes, abnormal traffic patterns, integrity check failures, and unexpected service restarts are recorded and made available for centralized analysis.

Monitoring functions are implemented in a standardized, machine-readable format suitable for integration with video management systems, centralized monitoring platforms, or security event analysis tools operated by the IOO. Where resource constraints prevent continuous local analysis on field devices, monitoring data is forwarded to upstream systems (e.g., VMS, TMC monitoring infrastructure) for correlation and alerting.

Parameter Value(s):

paragraph a.1. "Detect intrusion attempts, malware activity, unauthorized configuration changes, anomalous network traffic, and performance degradation"

paragraph b. "Network-based intrusion detection and prevention (IDPS) systems, host-based IDPS, Security Information and Event Management, file-integrity monitoring, anomaly detection, and log review/alerting."

paragraph g. #1 "Security event logs, IDPS alerts, authentication failures, configuration changes, vulnerability scan results, and incident response reports"

paragraph g. #2 "CISO, Security Admins, System Admins, and any other pertinent personnel or roles"

paragraph g. #3 "as needed and daily (automated), weekly (analyst review), and monthly (formal report)"

Risk References:

ATT&CK for ICS Mitigations / Techniques:

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

NIST SP 800-82⁽⁴⁾: The organization ensures that use of monitoring tools and techniques does not adversely impact the operational performance of the ITS. Example of compensating controls include deploying sufficient network, process, and physical monitoring.

ARC-IT Mechanisms:

- Each device shall have an adequate endpoint of malware detection and reporting system deployed. In most cases, a software suite of end point protections will include firewalls, anti-virus and malware detection, endpoint protection, reporting, and logging capabilities (among other features). Consider the capabilities when choosing a software suite and taking care to ensure 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/Prevention System (IPS) shall be configured to monitor data and detect malicious code signature in transit from all network infrastructure devices including routers, gateways, firewalls, load balancers, and switches.
- The IDS/IPS shall be configured to detect abnormalities in network activity compared to normal operation.
- The network will support centralized monitoring of all relevant security data.
- The IDS/IPS shall be updated regularly and tuned to properly report security incidents.
- A defined notification and response of policy and procedure shall be in place for relevant personnel to be informed and take action 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.

Standards: NIST SP 800-94⁽³⁴⁾, NIST SP 800-137⁽³⁵⁾

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

Responsible Party: M/I

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

Guidance: Inbound and outbound communications involving CCTV devices are monitored to detect unauthorized connections, protocol misuse, abnormal traffic patterns, and integrity violations.

Monitoring focuses on management interfaces, control channels, update mechanisms, and externally reachable services rather than raw video payload inspection, unless operationally justified. Where direct traffic inspection on the CCTV device is not feasible, traffic monitoring is performed at upstream network boundaries or aggregation points supporting the CCTV deployment.

Logging and reporting mechanisms provide sufficient detail to support incident investigation and correlation without capturing unnecessary payload data or degrading system performance.

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:

NIST SP 800-82⁽⁴⁾: 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(7), System Monitoring | Automated Response to Suspicious Events

Responsible Party: M/I

Justification to Select: Vulnerability "Intrusion detection and prevention software is not installed" in table 6, Policy and Procedure Vulnerabilities and Predisposing Conditions.

Guidance: Automated responses to suspicious events are limited to actions that do not disrupt critical surveillance or traffic safety operations.

Suspicious events trigger automated notifications to designated roles and systems, including centralized monitoring platforms or incident response personnel. Automated responses may include alert generation, session termination, interface throttling, or temporary isolation of affected services, provided such actions have been validated to avoid unintended operational impact.

Parameter Value(s):

paragraph a. "Security administrators, System Administrators"

paragraph b. "Send detailed event report to incident response personnel"

SI-4(14), System Monitoring | Wireless Intrusion Detection

Responsible Party: 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: For CCTV deployments that use wireless communications (e.g., Wi-Fi, licensed or unlicensed radio, cellular backhaul), monitoring mechanisms are employed to detect unauthorized wireless associations, rogue access points, and anomalous radio behavior.

Wireless intrusion detection may be implemented directly on the CCTV device where supported, or through external sensors, access points, or network monitoring systems covering the deployment area. Monitoring focuses on detecting unauthorized endpoints, unexpected protocol use, and signal anomalies indicative of spoofing or interception attempts.

SI-7, Software, Firmware, and Information Integrity

Responsible Party: M/I

Justification to Select: Threat "Compromise information systems or devices used externally and reintroduced into the enterprise" in table 3, Exploit and Compromise.

Threat "Conduct supply chain attacks targeting and exploiting critical hardware, software, or firmware" in table 3, Conduct an Attack (i.e., direct/coordinate attack tools or activities).

Vulnerability "Hardware, firmware, and software are not under configuration management" in Table 6, Configuration and Maintenance Vulnerabilities and Predisposing Conditions.

Guidance: CCTV systems implement integrity protections to ensure that software, firmware, configuration data, and stored video information have not been altered in an unauthorized or unexpected manner.

Integrity mechanisms apply to camera firmware, camera control and viewing software, boot components, configuration files, and stored or cached video data where feasible. Integrity verification is performed using cryptographic mechanisms (e.g., digital signatures, cryptographic hashes) anchored in hardware or protected storage where supported.

Integrity checks are designed to occur at well-defined lifecycle events such as device startup, reboot, firmware update, or configuration change. Continuous or intrusive integrity verification techniques are avoided on field-deployed devices unless they have been demonstrated not to interfere with operational performance.

When an integrity violation is detected, the CCTV system responds in a controlled manner appropriate to the severity of the violation. Responses may include logging the event, notifying designated personnel, restricting affected functionality, restarting the device into a known-good state, or shutting down non-essential services. Response actions are implemented to preserve traffic monitoring and safety functions wherever possible.

Parameter Value(s):

- paragraph a. "camera control and viewing software, camera firmware, and video data"
- paragraph b. "Shut down or restart device, Log incident, Report to Security Administrator"

Risk References:

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⁽⁴⁾: 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 modifications per IA-2.
- The device should support the integrity checks specified in NIST SP 800-147(25) 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-7(9) and SI-7(10).
- Approved mechanisms specific to dealing with integration of detection and response are specified in IR-4, IR-5.
- 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 restarting and shutting down and using 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

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

Guidance: Integrity checks are performed on defined software, firmware, and information elements at specific system states or events determined by the IOO.

The IOO defines which components require integrity verification and the events that trigger those checks, such as device startup, restart, firmware installation, or configuration changes. The manufacturer/vendor implements integrity-check mechanisms that align with these requirements and ensures that integrity verification does not degrade real-time video operations. Where integrity checks cannot be performed automatically due to system constraints, the system supports compensating controls such as periodic manual verification or controlled update processes,

Parameter Value(s):

#1 "camera control and viewing software, camera firmware, and video data"

#2 "At startup, restart"

Risk References:

NIST SP 800-82⁽⁴⁾: 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

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

Guidance: Integrity violations detected by CCTV components generate notifications and audit records sufficient to support timely investigation and response.

Notifications are transmitted to centralized monitoring or event management systems used by the IOO, or directly to designated roles where centralized systems are not available. Notification mechanisms provide sufficient context to identify the affected device, component, and nature of the integrity of failure without requiring direct access to the field device.

Where automated notification is not feasible due to deployment constraints, the system supports compensating procedures such as scheduled integrity status reviews, manual inspections, or maintenance reporting workflows.

Parameter Value(s):

"Security Admins, System Admins, and any other pertinent personnel or roles"

Risk References:

NIST SP 800-82⁽⁴⁾: In situations where the organization cannot employ automated tools that provide notification of integrity discrepancies, the organization employs non-automated mechanisms or procedures. Example of compensating controls include performing scheduled manual inspections for integrity violations.

ARC-IT Mechanisms: See SI-07.

SI-10, Information Input Validation

Responsible Party: M/I

Justification to Select: Threat "Spoofed reporting message" in table 3, Maintain a Presence or Set of Capabilities, and threat "Compromise mission-critical information" in table 3, Exploit and Compromise.

Guidance: CCTV systems validate all externally supplied inputs to prevent malformed, malicious, or unexpected data from affecting system operation, integrity, or availability. Input validation applies to management interfaces (e.g., web UI, CLI, APIs), control protocols, configuration files, firmware update packages, and network-based control or status messages.

Manufacturers implement server-side input validation using positive validation techniques appropriate to the interface and protocol, including strict bounds of checking, type enforcement, and rejection of malformed or unexpected protocol elements. For IP-based CCTV deployments, this includes validation of ONVIF, RTSP, HTTP(S), and vendor-specific management interfaces to ensure messages conform to protocol specifications and expected operational parameters.

Input size limits and parsing safeguards are enforced to prevent buffer overflows, memory corruption, and command injection. Validation logic is implemented within trusted execution contexts on the device and does not rely solely on upstream network protections. Input validation mechanisms are designed to fail safely, rejecting invalid input without disrupting active video capture or transmission.

Parameter Value(s):

"All inputs to web/application servers, database servers, and any system or application input that might receive a crafted exploit toward code/command execution or buffer overflow"

Risk References:

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

Justification to Select: Threat "Cause deterioration/destruction of critical information system components and functions" in table 3, Achieve Results (i.e., cause adverse impacts, obtain information), and threat "Cause integrity loss by polluting or corrupting critical data" in table 3, Achieve Results (i.e., cause adverse impacts, obtain information).

Guidance: CCTV systems protect memory used by operating systems, firmware, and applications to prevent exploitation techniques such as code injection, memory corruption, or unauthorized execution of data.

Manufacturers implement memory protection mechanisms supported by the device platform, prioritizing hardware-enforced protections where available. These mechanisms restrict execution of non-executable memory regions, randomize memory layout to reduce predictability, and prevent unauthorized modification of security-critical memory areas.

Parameter Value(s):

"Hardware-enforced data execution prevention and address space layout randomization"

Risk References:

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 implementation should be hardware-enforced.

SR Family – Supply Chain Risk Management

SR-2, Supply Chain Risk Management Plan

Responsible Party: M/I

Justification to Select: Threat "Conduct supply chain attacks targeting and exploiting critical hardware, software, or firmware" in table 3, Conduct an Attack (i.e., direct/coordinate attack tools or activities).

Guidance: The IOO establishes and maintains a supply chain risk management plan for CCTV systems that addresses risks associated with the acquisition, delivery, integration, and lifecycle support of hardware, firmware, and software components. The plan identifies critical CCTV components, defines risk acceptance criteria, and documents controls used to reduce exposure to counterfeit, tampered, or maliciously modified components.

Manufacturers are required to develop and provide a corresponding supply chain risk management plan covering their development, manufacturing, integration, and distribution processes for CCTV components. The plan is made available to the IOO for review and approval and updated as necessary when suppliers, manufacturing locations, or component sourcing changes. The level of

rigor applied is commensurate with the criticality of the CCTV deployment and the trustworthiness concerns associated with specific components.

Parameter Value(s):

- paragraph a. "key and/or critical system components"
- paragraph b. "at least annually"

SR-3, Supply Chain Controls and Processes

Responsible Party: 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 requires the CCTV manufacturer/vendor to establish documented supply chain controls and processes that protect against counterfeit, tampered, or unauthorized components entering the CCTV system. These processes address supplier selection, component traceability, secure handling during manufacturing and integration, and controls over distribution and delivery.

Parameter Value(s):

- paragraph a. #1 "key and/or critical system components"
- paragraph a. #2 Supply Chain Planners, Purchasing Managers, Inventory Controllers, Logistics Coordinators, and/or any other pertinent supply chain personnel.
- paragraph c. "security plan"

SR-6, Supplier Assessments and Reviews

Responsible Party: 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 may require the CCTV manufacturer/vendor to conduct periodic supplier assessments and reviews for suppliers providing critical or mission-essential CCTV components, such as cameras, encoders, processors, storage devices, or communication modules. These assessments evaluate supplier security practices, component authenticity controls, and resilience against tampering or malicious insertion.

Assessment results are documented and used to inform supplier selection, continued use, or risk mitigation actions. The depth and frequency of reviews are commensurate with the criticality of the supplied components and any known or emerging supply chain threats.

Parameter Value(s):

- "at least annually or as necessitated by security events or incidents."

SR-6(1), Supplier Assessments and Reviews | Testing and Analysis

Responsible Party: M/I

Justification to Select: Threats "Obtain information by opportunistically stealing or scavenging information systems/components" in table 3, Achieve Results (i.e., cause adverse impacts, obtain information).

Guidance: For selected critical CCTV components, the IOO may require independent testing or analysis to validate component integrity, authenticity, and conformance to security requirements. This may include hardware inspection, firmware analysis, or functional testing performed by qualified independent third parties.

Testing and analysis activities are targeted and risk-based, focusing on components where compromise could significantly impact system integrity, confidentiality, or operational availability.

Parameter Value(s):

#1 independent third-party analysis and independent third-party testing

SR-9, Tamper Resistance and Detection

Responsible Party: 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: Manufacturers design CCTV components, particularly cameras and roadside equipment, with tamper-resistance and tamper-evidence features appropriate for publicly accessible field environments. These features may include sealed or lockable enclosures, tamper-evident fasteners or seals, and intrusion detection mechanisms where feasible.

The IOO establishes inspection and response procedures for field personnel to identify signs of tampering and initiate corrective actions, such as reporting events to central operations, isolating affected devices, or initiating forensic review.

Risk References:

ATT&CK for ICS Mitigations / Techniques: M0947 / T0874, T0839, T0851, T0864

SR-10, Inspection of Systems or Components

Responsible Party (M/I): M/I

Justification to Select: Threats "Insert counterfeit or tampered hardware into the supply chain" and "Insert tampered critical components into organizational systems" in table 3, Deliver/Insert/Install Malicious Capabilities.

Guidance: The IOO implements procedures for inspecting CCTV systems and components throughout their operational lifecycle to verify integrity, detect tampering, and identify degradation or

unauthorized modification. Inspections may be conducted during installation, maintenance, and periodic field visits.

Manufacturers provide inspection guidance, indicators of compromise, and validation methods to support these inspections. Inspection results are documented and, where appropriate, recorded within TMC operational or security logs to support auditability and incident response.

SR-12, Component Disposal

Responsible Party: I

Justification to Select: Threats "Obtain information by opportunistically stealing or scavenging information systems/components" in table 3, Achieve Results (i.e., cause adverse impacts, obtain information).

Guidance: The IOO ensures that CCTV components and associated media are disposed of in a manner that prevents recovery of sensitive information, including video data and associated metadata that may contain PII. Prior to disposal or reuse, storage media is sanitized using approved methods appropriate to the media type and risk level.

Disposal activities are performed in accordance with organizational policies and applicable regulations, and may include media wiping, degaussing, physical destruction, or certified disposal services.

Parameter Value(s):

#1 "data stored on media storage devices"

#2 "disk cleaning or shredding"

Chapter 5. Implementation Considerations

Organizations should consider the following control guidance when implementing specific system capabilities when a system is used to store, process, or transmit ITS information.

PE-11, Emergency Power

Guidance: Loss of power to CCTV equipment can result in the loss of surveillance capability, situational awareness, or video evidence associated with traffic incidents. Emergency power capabilities should be implemented to support seamless transition and continued operation during power disruptions.

For transportation of CCTV systems, emergency power considerations typically include uninterruptible power supplies (UPS), battery-backed enclosures, connection to generator-supported circuits, or integration with existing ITS power resiliency infrastructure. This control should be applied to CCTV components whose availability supports broader ITS functions, such as incident detection, traffic monitoring, or coordinated response activities, with recovery objectives aligned to operational and safety needs rather than traditional IT uptime targets.

SC-5, Denial of Service Protection

Guidance: CCTV systems used in transportation environments are susceptible to denial-of-service (DoS) conditions caused by network congestion, excessive video streaming demands, storage saturation, or malicious traffic. Such conditions can degrade or interrupt video availability at critical times, potentially obscuring incidents or delaying responses.

Implementation of this control should focus on maintaining operational availability rather than preventing all forms of resource exhaustion. Practical measures include traffic rate limiting management interfaces, prioritization of essential video and control traffic, buffering or stream throttling under load, and monitoring mechanisms capable of detecting abnormal resource utilization. DoS protections should be designed to avoid disrupting normal CCTV operations.

SR-9, Tamper Resistance and Detection

Guidance: CCTV components are frequently deployed in exposed or publicly accessible roadside environments, making them vulnerable to physical tampering, vandalism, or unauthorized access. Physical compromise of a CCTV device can result in loss of video availability, unauthorized access to system interfaces, or manipulation of captured footage.

To mitigate these risks, tamper-resistance, and tamper-detection mechanisms such as lockable or sealed enclosures, tamper-evident fasteners, intrusion detection switches, or alarms should be integrated where

feasible. These mechanisms support preservation of system availability and integrity and complement procedural controls such as field inspections and centralized monitoring.

AC-18, Wireless Access

Wireless connectivity in transportation CCTV deployments is operationally complex and highly variable. CCTV systems may rely on Wi-Fi, cellular, licensed microwave, or other wireless links for video transport, management access, maintenance, or temporary deployments. These links often traverse uncontrolled or publicly accessible environments and may be intermittently available due to coverage gaps, weather, or mobility.

Implementation of wireless access controls should therefore focus on risk containment rather than simple enable/disable decisions. When wireless communications are used, safeguards such as strong encryption, mutual authentication, and integrity protection should be applied to all video, control, and management of traffic. Wireless configurations should prevent unauthorized association, limit exposure of management interfaces, and ensure that loss or degradation of the wireless link does not place the CCTV device into an unsafe or insecure state.

Where cellular connectivity is used, organizations should not assume that carrier-provided protections are sufficient. Application-layer protections (e.g., VPNs, certificate-based authentication, encrypted tunnels) remain relevant to protect against interception, misrouting, or unauthorized access. Wireless security mechanisms must be selected and tuned to avoid introducing instability or latency that could impair CCTV operations, consistent with NIST SP 800-82 guidance for OT systems.

CM-7(8), Least Functionality | Binary or Machine Executable Code

This control enhancement addresses the risks associated with executable code present within CCTV systems, including camera firmware, video processing software, management applications, and embedded operating systems. Such code may originate from commercial vendors, open-source components, or third-party libraries.

Transportation CCTV components may have limited or fixed functionality, but when executable code is present, it can significantly affect the system's risk of posture. Implementation of this enhancement should focus on minimizing unnecessary executable code, disabling unused services, and ensuring that only required software and firmware are installed and enabled. These measures should be applied in a manner that supports intended operational capabilities while reducing attack surface and aligning with the least functionality principles appropriate for ITS and OT environments.

SC-17 Public Key Infrastructure and Certificate Use

Guidance: Transportation CCTV systems increasingly depend on cryptographic identity to support secure communications, remote management, and integration with ITS infrastructure. Implementation of PKI should account for the mixed operational environment in which CCTV devices operate, including both roadside and enterprise contexts.

Manufacturers and operators may support multiple certificate frameworks depending on the use case. For example, IEEE 1609.2 / SCMS-based credentials may be appropriate for edge or field-facing connectivity within ITS ecosystems, while X.509-based PKI may be more suitable for centralized management, maintenance access, or integration with enterprise security systems. Supporting both approaches

provides flexibility, allowing the IOO to select the certificate model that best aligns with operational architecture and trust relationships.

Enrollment, provisioning, and renewal processes should be designed to function securely in constrained or intermittently connected environments, such as roadside deployments. Certificate lifecycle management should minimize manual handling, avoid service disruption, and support revocation or replacement when devices are compromised, retired, or reassigned. These considerations complement, but do not replace cryptographic key protection requirements addressed elsewhere in the control set.

Appendix A. Threats, Vulnerabilities, and Predisposing Conditions

A broad set of adversarial and non-adversarial threat events that could potentially impact CCTV is provided in Table 3 (adversarial) and Table 4 (non-adversarial) below. The properties of CCTV may also present unique opportunities to a threat source, specifically addressing how the threat source can manipulate the process of the CCTV or the supported service package to cause physical damage. Table 5 provides an overview of potential threat events more specific to the CCTV. Threat events listed below focus on the CCTV, not the larger system comprised of various types of physical objects and other components. Various threat events may ultimately impact a CCTV or its mission/operations, either by compromise of the CCTV 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 CCTV can implement a protection measure to mitigate the risk will the threat be considered relevant to the CCTV itself and, therefore, controls will be selected in this document to mitigate only those risks.

Table 3. Adversarial Threat Events

Threat Events	Tactics, Techniques, and Procedures	Description
<i>Perform Reconnaissance and Gather Information</i>	Perform perimeter network reconnaissance/scanning.	Adversary uses commercial or free software to scan organizational perimeters to obtain a better understanding of the information technology infrastructure.
	Perform network sniffing of exposed networks.	Adversary with access to exposed wired or wireless data channels used to transmit information, uses network sniffing to identify components, resources, and protections. CCTV systems core communication could be compromised, affecting the confidentiality, integrity, and availability of the device.

Threat Events	Tactics, Techniques, and Procedures	Description
	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>Deliver/Insert/Install Malicious Capabilities</i>	Insert counterfeit or tampered hardware into the supply chain.	Adversary intercepts hardware from legitimate suppliers. Adversary modifies CCTV' hardware or replaces it with faulty or otherwise modified hardware.
	Insert tampered critical components into CCTV systems.	Adversary replaces, through supply chain, subverted insider, or some combination thereof, critical information system components with modified or corrupted components.
	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 persistent and targeted sniffers on organizational information systems and networks.	Adversary places within internal organizational information systems or networks software designed to (over a continuous period of time) collect (sniff) network traffic.
<i>Exploit and Compromise</i>	Exploit recently discovered vulnerabilities.	Adversary exploits recently discovered vulnerabilities in CCTV internal information systems in an attempt to compromise the systems before mitigation measures are available or in place.
	Exploit vulnerabilities on CCTV internal information systems.	Adversary searches for known vulnerabilities in CCTV internal information systems and exploits those vulnerabilities.

Threat Events	Tactics, Techniques, and	Description
	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.
	Exploit poorly configured or unauthorized information systems exposed to the Internet.	<TODO>
	Compromise critical systems via physical access.	Adversary obtains physical access to organizational information systems and makes modifications.
	Compromise design, manufacture, and/or distribution of CCTV information system components (including hardware, software, and firmware).	Adversary compromises the design, manufacture, and/or distribution of critical information system components at selected suppliers.
	Compromise CCTV information systems to facilitate exfiltration of data/information.	Adversary malware into internal CCTV information systems, where the malware over time can identify and then exfiltrate valuable information.
	Compromise software of organizational critical information systems.	Adversary inserts malware or otherwise corrupts critical internal organizational information systems.
	Compromise information systems or devices used externally and reintroduced into the enterprise.	Adversary installs malware on information systems or devices while the systems/devices are external to organizations for purposes of subsequently infecting organizations when reconnected.
	Compromise mission-critical information.	Adversary compromises the integrity of mission-critical information, thus preventing or impeding the ability of organizations to which information is supplied, from carrying out operations.

Threat Events	Tactics, Techniques, and	Description
Conduct an Attack (i.e., direct/coordinate attack tools or activities)	Conduct communications interception attacks.	Adversary takes advantage of communications that are either unencrypted or use weak encryption (e.g., encryption containing officially 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 on critical information systems, components, or supporting infrastructures, based on adversary knowledge of dependencies.
	Conduct externally based network traffic modification (man in the middle) attacks.	Adversary, operating outside organizational systems, intercepts/eavesdrops on sessions between organizational and external systems. Adversary then relays messages between organizational and external systems, making them believe that they are talking directly to each other over a private connection, when in fact the entire communication is controlled by the adversary. Such attacks are of particular concern for organizational use of community, hybrid, and public clouds.
	Conduct externally based session hijacking.	<TODO>

Threat Events	Tactics, Techniques, and Procedures	Description
	Conduct internally-based network traffic modification (man in the middle) attacks.	Adversary operating within the organizational infrastructure intercepts and corrupts data sessions.
	Conduct supply chain attacks targeting and exploiting critical hardware, software, or firmware.	Adversary targets and compromises the operation of software (e.g., through malware injections), firmware, and hardware that perform critical functions for organizations. This is accomplished as supply chain attacks on both commercial off-the-shelf and custom information systems and components.
	Conduct brute force login attempts/password guessing attacks.	<TODO>
<i>Achieve Results (i.e., cause adverse impacts, obtain information)</i>	Obtain sensitive information through network sniffing of external networks.	Adversary with access to exposed wired or wireless data channels that organizations (or organizational personnel) use to transmit information (e.g., kiosks, public wireless networks) intercepts communications.
	Cause integrity loss by polluting or corrupting critical data.	Adversary implants corrupted and incorrect data in critical data, resulting in suboptimal actions or loss of confidence in organizational data/services.
	Cause deterioration/destruction of critical information system components and functions.	Adversary destroys or causes deterioration of critical information system components to impede or eliminate organizational ability to carry out missions or business functions. Detection of this action is not a concern.
	Obtain unauthorized access.	Adversary with authorized access to organizational information systems, gains access to resources that exceed authorization.

Threat Events	Tactics, Techniques, and Procedures	Description
	Obfuscate adversary actions.	Adversary takes actions to inhibit the effectiveness of the intrusion detection systems or auditing capabilities within organizations.
	Obtain sensitive information via exfiltration.	Adversary directs malware on organizational systems to locate and surreptitiously transmit sensitive information.
	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.
Coordinate a Campaign	Coordinate cyberattacks using external (outsider), internal (insider), and supply chain (supplier) attack vectors.	Adversary employs continuous, coordinated attacks, potentially using all three attack vectors for the purpose of impeding organizational operations.
Craft or Create Attack Tools	Create and operate false front organizations to inject malicious components into the supply chain.	Adversary creates false front organizations with the appearance of legitimate suppliers in the critical lifecycle path that then inject corrupt/malicious information system components into the organizational supply chain.

Table 4 provides a high-level characterization of non-adversarial threat events as adapted from NIST SP 800-30.⁽³⁾ 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 with exceptional privileges or sets privilege requirements on a resource too low.
Spill sensitive information.	Authorized users erroneously contaminate a device, information system, or network by placing it or sending

Threat Event	Description
	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.
Mishandling of critical and/or sensitive information by authorized users.	Authorized privileged user for critical/sensitive information.
Earthquake at primary location.	Earthquake of organization-defined magnitude at primary locations makes location inoperable.
Fire at the primary location.	Fire (not due to adversarial activity) at primary locations makes location inoperable.
Fire at backup location.	Fire (not due to adversarial activity) at a 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 organization-defined strength at primary location makes location inoperable.
Hurricane at backup location.	Hurricane 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.

Threat Event	Description
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 5 provides an overview of potential threat events that are specific to and even more relevant to the CCTV than the general threats listed in table 3 and table 4. These physical object threat events are adapted from NIST SP 800-82⁽⁴⁾ 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 vulnerabilities and predisposing conditions from NIST SP 800-82.⁽⁴⁾ 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
Policy and Procedure Vulnerabilities and Predisposing Conditions	Inadequate ITS security training and awareness program.	A documented formal ITS security training and awareness program is designed to keep staff up to date on organizational security policies and procedures, threats, industry cybersecurity standards, and recommended practices. Without adequate ongoing training on specific ITS policies and procedures, staff cannot be expected to maintain a secure ITS environment.
	Inadequate security policy for ITS.	Vulnerabilities are often introduced into the OT environment due to inadequate policies or the lack of policies specifically for OT system security. Controls and countermeasures should be derived from a risk assessment or policy to ensure uniformity and accountability.
	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.
	Hardware, firmware, and software not under asset management.	The organization does not know the patch 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.

Vulnerability		Description
	Lack of configuration management policy.	Lack of policy and procedures for ITS configuration management can lead to an unmanageable and highly vulnerable inventory of hardware, firmware, and software.
	Lack of redundancy for critical components.	Lack of redundancy in critical components could provide single-point-of failure possibilities.
	Inadequate incident detection and 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 anomalies, prioritizing the handling of incidents, and implementing effective methods of collecting, analyzing, and reporting data.
	Malware protection was implemented without sufficient testing.	Malware protection software that is deployed without sufficient testing could impact normal operation of the OT and block the system from performing necessary control actions.
Architecture and Design Vulnerabilities and Predisposing Conditions	No security perimeter is defined.	If the OT does not have a security perimeter clearly defined, it is not possible to ensure that the necessary security controls are deployed and configured properly. This can lead to unauthorized access to systems and data, as well as other problems.
	Control networks are 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 non-control traffic to the control of traffic, which could lead to hijacking or other types of attacks.
	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

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

Vulnerability		Description
		also needed to identify problems with controls, such as misconfiguration and failures.
Configuration and Maintenance Vulnerabilities and Predisposing Conditions	Hardware, firmware, and software are not under asset management.	The organization doesn't know what it has (e.g., make, model), where they are, or what version it has, resulting in an inconsistent and ineffective defense posture. To properly secure an ITS, there should be an accurate inventory of the assets in the environment. Procedures should be in place to manage additions, deletions, and modifications of assets which include asset inventory management. These procedures are critical to executing business continuity and disaster recovery plans.
	Hardware, firmware, and software are not under configuration management.	The organization does not know the patch 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.
	Operating system and vendor software patches may not be developed until long after security vulnerabilities are found.	Out-of-date operating systems and applications may contain newly discovered vulnerabilities that could be exploited. Security patch support may not be available for legacy OT, so vulnerability management procedures should include contingency plans for mitigating vulnerabilities where patches may never be available or replacement plans.
	Critical configurations are not stored or backed up.	<TODO>
	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

Vulnerability		Description
		individuals from gaining access or authorized individuals from gaining excessive access to the OT.
	Poor configurations are used	<TODO>
	Inadequate access controls applied.	Access controls must be matched to the way the organization allocates responsibilities and privilege to its personnel. Poorly specified access controls can result in giving an ITS user too many or too few privileges. The following exemplify each case: • System configured with default access control settings gives an operator administrative privileges. • System configured improperly results in an operator being unable to take corrective actions in an emergency.
	Malware protection is not installed or up to date.	For physical objects that include an operating system and possibly applications, installation of malicious software, or malware, is a common attack. Malware protection software, such as antivirus software, should be kept current in a very dynamic environment. Outdated malware protection software and definitions leave the system open to malware threats.
	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.
	Lack of a vulnerability management program.	Vulnerabilities not considered by the organization could result in exploitation. Vulnerability management procedures should be in place to determine a plan of action or inaction upon the discovery of a vulnerability. Some OT considerations are availability concerns may push patching until the next planned operational downtime; security patch support may not be available for OT systems that use outdated operating systems; isolated systems may not require immediate patching; and OT exposed to the internet may need to be prioritized for patching.

Vulnerability		Description
	Intrusion detection and prevention software is not installed.	Incidents can result in loss of system availability and integrity; the capture, modification, and deletion of data; and incorrect execution of control commands. Intrusion detection system/intrusion protection system software may stop or prevent various types of attacks, including DoS attacks, and also identify attacked internal hosts, such as those infected with worms. Intrusion detection system/intrusion protection system software must be tested prior to deployment to ensure that it does not compromise normal operation of the OT.
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, EMP, static discharge, brownouts, and voltage spikes.	Some hardware used for OT systems is vulnerable to radio frequency, EMPs, static discharge, brownouts, and voltage spikes. The impacts can range from the temporary disruption of command and control to permanent damage to circuit boards. Proper shielding, grounding, power conditioning, and/or surge suppression are recommended.
	Lack of backup power.	Without backup power to critical assets, a general loss of power will shut down the OT and could create an unsafe situation. Loss of power could also lead to insecure default settings. If the program file or data is stored in volatile memory, the process may not be able to restart after a power outage without appropriate backup power.

Vulnerability		Description
	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 them 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, FTP, HTTP, and Network File System. The use of such protocols also makes it easier for adversaries to perform attacks against the OT and manipulate OT network activity.
	Use of unsecure OT protocols.	OT protocols often have few or no security capabilities, such as authentication and encryption, to protect data from unauthorized access or tampering. The incorrect implementation of the protocols can also lead to additional vulnerabilities.
	Lack of integrity checking for communications.	Integrity checks are not built into most OT protocols, so adversaries could manipulate communications undetected. To ensure integrity, the OT can use lower-layer protocols (e.g., IPsec) that offer data integrity protection when traversing untrusted physical media.
	Authentication of users, data, or devices is substandard or nonexistent.	<TODO>

Vulnerability		Description
	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 authentication between clients and servers over wireless connections.	<TODO>
	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 unencrypted data.
	Inappropriate segmentation of the asset management system.	Most architectures are designed for PLCs, remote terminal units, distributed control systems, and SCADA controllers to manipulate the process and for asset management systems to monitor the assets connected to the controllers. Many asset management systems also have the technical ability to modify the configuration of sensors and final elements, although modification may not be their primary function. The asset management system should be controlled appropriately based on its ability (or lack of ability) to manipulate the process.
Sensor, Final Element, and Asset Management Vulnerabilities and Predisposing Conditions	Unauthorized physical access to sensors or final elements.	Physical access to sensors and final elements allows for direct manipulation of the physical process. Many smart devices are configured on a fieldbus such that electronic access to the sensor network allows for manipulation of controlling parameters. Physical access to the whole loop should be managed to prevent incidents.
	Unauthorized wireless access to sensors or final elements.	Wireless access to sensors and final elements allows for direct manipulation of the physical process. Many smart devices allow for wireless configuration. Wireless access should be securely configured or disabled using hardware write-protect where possible to protect unauthorized modification of the sensors and final elements which are connected both to the physical process and to the physical object environment.

Vulnerability		Description
	Inappropriate segmentation of asset management systems.	Most architectures are designed for PLCs, remote terminal units, distributed control systems, and SCADA controllers to manipulate the process, and for asset management systems to monitor the assets connected to the controllers. Many asset management systems also have the technical ability to modify the configuration of sensors and final elements, although modification may not be their primary function. The asset management system should be controlled appropriately based on its ability (or lack of ability) to manipulate the process.

Appendix B. NIST SP 800-53 Security Control's Mapping

Table 7. Mapping of CCTV 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	
	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.	3	MA-01: Policy and Procedures MP-01: Policy and Procedures PE-01: Policy and Procedures PL-01: Policy and Procedures	MA-1 was not chosen because maintenance policies are set at the organizational level. MP-1 was not chosen because media protection policies are managed at the enterprise level,

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	with CCTV video streams handled by centralized ITS storage solutions, negating the need for device-level policy enforcement. PE-1 was not chosen because physical and environmental protection policies are administered organizationally. PL-1 was not chosen because security planning policies are crafted at the enterprise level. PM-1 was not chosen because information security program policies are defined organizationally. PS-1 was not chosen because personnel security policies are low priority for CCTV systems, which have minimal direct operator access. PS-1 was not chosen because personnel security policies are low priority for CCTV systems, which have minimal direct operator access. RA-1 was not chosen because risk assessment policies are a lower priority for CCTV, controls emphasizing physical and network vulnerabilities are a higher focus than broad procedural assessments.

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
				SA-1 was not chosen because system and services acquisition policies are organizational and not device-specific for CCTV. SC-1 was not chosen because system and communications protection policies are covered by technical controls like encryption for CCTV video transmission. SI-1 was not chosen because system integrity policies are low priority, with CCTV integrity maintained through hardware checks and network monitoring. PM-28 was not chosen because risk framing is an enterprise-level process, integrated into overall ITS risk management rather than CCTV-specific.
	GV.OC-04: Critical objectives, capabilities, and services that external stakeholders depend on or expect from the organization are understood and communicated.	3	PM-08: Critical Infrastructure Plan PM-11: Mission and Business Process Definition CP-02(08): Identify Critical Assets PM-30(01): Suppliers of Critical or Mission-Essential Items RA-09: Criticality Analysis	PM-8 was not chosen because critical infrastructure planning is addressed at the broader transportation network level, not for stand-alone CCTV systems. RA-09 was not chosen because criticality analysis for mission-essential functions is conducted at the ITS portfolio level, not for specific CCTV instances, to prioritize resources across transportation assets.

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
	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 CCTV deployment in the field.
	GV.RM-01: Risk management objectives are established and agreed to by organizational stakeholders.	3	PM-09: Risk Management Strategy RA-07: Risk Response SR-02: Supply Chain Risk Management Plan	
	GV.RM-05: Lines of communication across the organization are established for cybersecurity risks, including risks from suppliers and other third parties.	3	PM-09: Risk Management Strategy PM-30: Supply Chain Risk Management Strategy	
	GV.RM-06: A standardized method for calculating, documenting, categorizing, and prioritizing cybersecurity risks is established and communicated.	3	PM-09: Risk Management Strategy PM-18: Privacy Program Plan PM-28: Risk Framing PM-30: Supply Chain Risk Management Strategy RA-03: Risk Assessment	PM-18 was not chosen because while CCTV may capture potential PII, privacy program planning is managed centrally in ITS, not at the device level where video is primarily for traffic monitoring.
	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	

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
			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-19 was not chosen because privacy leadership roles are organizational and not applicable to CCTV systems, which handle video data under broader privacy governance. PM-23 was not chosen because data governance is low priority for CCTV, which generates video streams managed by central ITS data policies rather than requiring a dedicated body. PM-24 was not chosen because data integrity oversight for CCTV video feeds is ensured through technical transmission controls, not necessitating a formal board. PM-29 was not chosen because risk management leadership is organizational, with CCTV risks incorporated into wider 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	PM-11 was not chosen because mission and business process definitions are organizational, with CCTV serving supportive monitoring functions within defined ITS processes.

Objective	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
			SR-05: Acquisition Strategies, Tools, and Methods	
	GV.SC-01: A cybersecurity supply chain risk management program, strategy, objectives, policies, and processes are established and agreed to by organizational stakeholders.	3	PM-30: Supply Chain Risk Management Strategy SR-02: Supply Chain Risk Management Plan SR-03: Supply Chain Controls and Processes	
	GV.SC-03: Cybersecurity supply chain risk management is integrated into cybersecurity and enterprise risk management, risk assessment, and improvement processes.	3	AC-01: Policy and Procedures AT-01: Policy and Procedures AU-01: Policy and Procedures CA-01: Policy and Procedures CM-01: Policy and Procedures CP-01: Policy and Procedures IA-01: Policy and Procedures IR-01: Policy and Procedures MA-01: Policy and Procedures MP-01: Policy and Procedures PE-01: Policy and Procedures PL-01: Policy and Procedures 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	AT-1 was not chosen because it focuses on developing organizational-level security awareness and training policies, which are less critical for CCTV systems that operate with minimal human interaction and limited user training needs. AU-1 was not chosen because audit and accountability policies are low priority for CCTV, as logging is handled by network-level systems rather than device-specific procedures. CA-1 was not chosen because security assessment policies are organizational and integrated into broader ITS evaluations, not tailored for individual CCTV deployments with focused video streaming functions. CM-1 was not chosen because configuration management.

Objective	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
			SI-01: Policy and Procedures SR-01: Policy and Procedures PM-09: Risk Management Strategy PM-18: Privacy Program Plan PM-30: Supply Chain Risk Management Strategy PM-31: Continuous Monitoring Strategy SR-02: Supply Chain Risk Management Plan SR-03: Supply Chain Controls and Processes RA-03: Risk Assessment RA-07: Risk Response	policies are established organizationally. Additional CM controls are applied to the CCTV to ensure configuration management. CP-1 was not chosen because contingency planning policies are organizational, with CCTV redundancy addressed through ITS-wide recovery strategies rather than device-level policies. IA-1 was not chosen because identification and authentication are implemented enterprise-wide and do not require device-level policies. IR-1 was not chosen because incident response policies are implemented enterprise-wide and do not require device-level policies. PM-31 was not chosen because Continuous Monitoring Strategy are implemented enterprise-wide and do not require device-level policies.
	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	

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	SA-04: Acquisition Process SA-09: External System Services SR-03: Supply Chain Controls and Processes SR-05: Acquisition Strategies, Tools, and Methods SR-06: Supplier Assessments and Reviews SR-10: Inspection of Systems or Components	
	GV.SC-06: Planning and due diligence are performed to reduce risks before entering into formal supplier or other third-party relationships.	3	SA-04: Acquisition Process SA-09: External System Services SR-05: Acquisition Strategies, Tools, and Methods SR-06: Supplier Assessments and Reviews	
	GV.SC-07: The risks posed by a supplier, their products, and services, and other third parties are understood, recorded, 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	3	PM-09: Risk Management Strategy PM-19: Privacy Program Leadership Role PM-28: Risk Framing	

Objective	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
	the technology product and service lifecycle.		PM-30: Supply Chain Risk Management Strategy PM-31: Continuous Monitoring Strategy RA-03: Risk Assessment RA-07: Risk Response SA-04: Acquisition Process SA-09: External System Services SR-02: Supply Chain Risk Management Plan SR-03: Supply Chain Controls and Processes SR-05: Acquisition Strategies, Tools, and Methods SR-06: Supplier Assessments and Reviews	
	GV.SC-10: Cybersecurity supply chain risk management plans include 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	

Objective	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
			SR-06: Supplier Assessments and Reviews	
	ID.AM-01: Inventories of hardware managed by the organization are maintained.	3	CM-08: System Component Inventory PM-05: System Inventory	
	ID.AM-02: Inventories of software, services, and systems managed by the organization are maintained.	3	AC-20: Use of External Systems CM-08: System Component Inventory PM-05: System Inventory SA-05: System Documentation SA-09: External System Services	PM-22 was not chosen because CCTV in ITS focuses on real-time traffic surveillance without long-term PII storage or processing, making quality management controls unnecessary at the device level.
	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 was not chosen because PII quality operations are irrelevant for CCTV, as traffic monitoring video is not processed for PII extraction or quality assurance at the device level. SA-03 was not chosen because integrating security into the system development lifecycle is moderate priority but managed during ITS system design, not CCTV alone. SI-12 was not chosen because log based controls within this document covers the management and retention of information.

Objective	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
			SI-18: Personally Identifiable Information Quality Operations SR-05: Acquisition Strategies, Tools, and Methods SR-12: Component Disposal	CM-9 is addressed at the broader ITS system level to ensure consistent configuration management across all components, making a specific CCTV plan redundant.
	ID.RA-04: Potential impacts and likelihoods of threats exploiting vulnerabilities are identified and recorded.	3	PM-09: Risk Management Strategy PM-11: Mission and Business Process Definition RA-02: Security Categorization RA-03: Risk Assessment RA-08: Privacy Impact Assessments RA-09: Criticality Analysis	RA-02 was not chosen because security categorization of the overall ITS system, including CCTV, is performed at the program level rather than per device to align with federal categorization standards.
	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 CCTV monitoring systems.
	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	

Objective	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
	ID.RA-10: Critical suppliers are assessed prior to acquisition.	3	SR-06: Supplier Assessments and Reviews	
	ID.IM-01: Improvements are identified from evaluations.	3	AC-01: Policy and Procedures AT-01: Policy and Procedures AU-01: Policy and Procedures CA-01: Policy and Procedures CM-01: Policy and Procedures CP-01: Policy and Procedures IA-01: Policy and Procedures IR-01: Policy and Procedures MA-01: Policy and Procedures MP-01: Policy and Procedures PE-01: Policy and Procedures PL-01: Policy and Procedures PM-01: Information Security Program Plan PS-01: Policy and Procedures PT-01: Policy and Procedures RA-01: Policy and Procedures SA-01: Policy and Procedures SC-01: Policy and Procedures SI-01: Policy and Procedures SR-01: Policy and Procedures CA-02: Control Assessments CA-05: Plan of Action and Milestones CA-07: Continuous Monitoring CA-08: Penetration Testing	CA-2 was not chosen because periodic control assessments are moderate priority but conducted at the ITS network level, not requiring device-specific evaluations for CCTV's real-time monitoring role. SA-17(6) was not chosen because testing structures in development are not necessary for CCTV operations, focusing instead on integration testing within ITS networks. CP-02 was not chosen since other CP controls (CP-9 & CP-10) were selected to provide sufficient coverage for unpredicted circumstances.

Objective	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
			CP-02: Contingency Plan IR-04: Incident Handling IR-08: Incident Response Plan PL-02: System Security and Privacy Plans RA-03: Risk Assessment RA-05: Vulnerability Monitoring and Scanning RA-07: Risk Response SA-08: Security and Privacy Engineering Principles SA-11: Developer Testing and Evaluation SA-17(06): Structure For Testing SI-02: Flaw Remediation SI-04: System Monitoring SR-05: Acquisition Strategies, Tools, and Methods	
	ID.IM-02: Improvements are identified from security tests and exercises, including those done in 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,	3	CP-02: Contingency Plan IR-08: Incident Response Plan PL-02: System Security and Privacy Plans	CP-2 was not chosen because detailed contingency plans are less critical for CCTV, which can leverage overlapping camera

Objective	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
	communicated, maintained, and improved.		SR-02: Supply Chain Risk Management Plan	coverage and central system backups for continuity.
	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 incorporate the principles of least privilege and separation of duties.	2	AC-03: Access Enforcement AC-05: Separation of Duties AC-06: Least Privilege AC-17: Remote Access 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 CCTV devices in ITS have limited direct human interaction, diminishing the need for extensive literacy training programs beyond basic maintenance protocols.

Objective	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
	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	
	PR.PS-05: Installation and execution of unauthorized software are prevented.	3	CM-07(02): Prevent Program Execution CM-07(04): Unauthorized Software — Deny by Exception CM-07(05): Authorized Software — Allow by Exception SC-34: Non-Modifiable Executable Programs	SC-34 was not chosen because CCTV firmware is designed to be non-modifiable in the field via physical enclosures and access controls, aligning with this control inherently without additional specifications.
	PR.IR-02: The organization's technology 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	SI-13 was not chosen because SC-24 Fail in Known State provides sufficient guidance for securing failures to the CCTV system.

Objective	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
	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	PM-3 was not chosen because resource allocation for security and privacy is managed at the program level, not allocated specifically for CCTV 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 with relevant	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
	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 CCTV units.
	RS.MA-02: Incident reports are triaged and validated.	3	IR-04: Incident Handling IR-05: Incident Monitoring IR-06: Incident Reporting	
	RS.MA-03: Incidents are categorized and prioritized.	3	IR-04: Incident Handling IR-05: Incident Monitoring IR-06: Incident Reporting	
	RS.MA-04: Incidents are escalated or elevated as needed.	3	IR-04: Incident Handling IR-05: Incident Monitoring IR-06: Incident Reporting IR-07: Incident Response Assistance	IR-07 was not chosen because this control pertains to providing assistance during incidents across the organization, which is handled by centralized ITS support teams rather than decentralized CCTV field equipment.
	RS.MA-05: The criteria for initiating incident recovery are applied.	3	IR-04: Incident Handling IR-08: Incident Response Plan	IR-08 was not chosen because a comprehensive incident response plan is developed and maintained at the ITS system level, not for isolated CCTV devices, to ensure coordinated response across the transportation infrastructure.
	RS.MI-01: Incidents are contained.	3	IR-04: Incident Handling	

Objective	Subcategory	Affinity Score	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	

Objective	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
Mission Objective #3: Collect, Manage, Use, and Disseminate Data	GV.OC-02: Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered.	3	Subcategory/Security Controls are covered in Mission Objective 1	
	GV.OC-03: Legal, regulatory, and contractual requirements regarding cybersecurity—including privacy and civil liberties obligations—are understood and managed.	3	Subcategory/Security Controls are covered in Mission Objective 1	
	GV.OC-04: Critical objectives, capabilities, and services that external stakeholders depend on or expect from the organization are understood and communicated.	3	Subcategory/Security Controls are covered in Mission Objective 1	
	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	

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-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	
	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	

Objective	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
	GV.SC-09: Supply chain security practices are integrated into cybersecurity and enterprise risk management programs, and their performance is monitored throughout the technology product and service lifecycle.	3	Subcategory/Security Controls are covered in Mission Objective 1	
	GV.SC-10: Cybersecurity supply chain risk management plans include provisions for activities that occur after the conclusion of a partnership or service agreement.	3	Subcategory/Security Controls are covered in Mission Objective 1	
	ID.AM-03: Representations of the organization's authorized network communication and internal and external network data flows are maintained.	3	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 handled during ITS system design, not as a control for operational CCTV units.
	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	
	ID.AM-08: Systems, hardware, software, services, and data are managed throughout their lifecycles.	3	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-

Objective	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
				28 (Protecting of Information at Rest).
	ID.RA-01: Vulnerabilities in assets are identified, validated, and recorded.	3	CA-02: Control Assessments CA-07: Continuous Monitoring CA-08: Penetration Testing RA-03: Risk Assessment RA-05: Vulnerability Monitoring and Scanning SA-11(02): Threat Modeling and Vulnerability Analyses SA-15(07): Automated Vulnerability Analysis SA-15(08): Reuse of Threat and Vulnerability Information SI-04: System Monitoring SI-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	

Objective	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
	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-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	
	PR.AA-02: Identities are proofed and bound to credentials based on the context of interactions.	2	IA-12: Identity Proofing	

Objective	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
	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	
	PR.AA-05: Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties.	3	AC-01: Policy and Procedures AC-02: Account Management AC-03: Access Enforcement AC-05: Separation of Duties AC-06: Least Privilege AC-10: Concurrent Session Control AC-16: Security and Privacy Attributes AC-17: Remote Access AC-18: Wireless Access AC-24: Access Control Decisions IA-13: Identity Providers and Authorization Servers	IA-13 was not added to the list of security controls since it was withdrawn from NIST SP 800-53r5. Did not include AC-19: <i>Access Control For Mobile Devices</i> due to it's not being applicable to the CCTV system.

Objective	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
	PR.AT-01: Personnel are provided with awareness and training so that they possess the knowledge and skills to perform general tasks with cybersecurity risks in mind.	3	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 SI-03: Malicious Code Protection SI-04: System Monitoring SI-07: Software, Firmware, and Information Integrity	SC-12 was not chosen because key management for CCTV encryption is handled by the central TMC or network infrastructure, not locally on the device, to centralize cryptographic operations and reduce field complexity.
	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	

Objective	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
			SC-07: Boundary Protection SC-08: Transmission Confidentiality and Integrity SC-11: Trusted Path SC-12: Cryptographic Key Establishment and Management SC-13: Cryptographic Protection SC-16: Transmission of Security and Privacy Attributes SC-40: Wireless Link Protection SC-43: Usage Restrictions SI-03: Malicious Code Protection SI-04: System Monitoring SI-07: Software, Firmware, and Information Integrity	
	PR.DS-10: The 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.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 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	

Objective	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
			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	AC-03: Access Enforcement AC-04: Information Flow Enforcement SC-04: Information In Shared System Resources SC-05: Denial-of-Service Protection SC-07: Boundary Protection	
	PR.IR-03: Mechanisms are implemented to achieve resilience requirements in normal and adverse situations.	3	Subcategory/Security Controls are covered in Mission Objective 1	
	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 CM-06: Configuration Settings CM-10: Software Usage Restrictions CM-11: User-Installed Software	

Objective	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
			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 assets is verified before using them for restoration.	3	CP-02: Contingency Plan CP-04: Contingency Plan Testing CP-09: System Backup	

Objective	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
	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	CP-10: System Recovery and Reconstitution	
CP-10: System Recovery and Reconstitution	GV.OC-02: Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered.	3	Subcategory/Security Controls are covered in Mission Objective 1	
	GV.OC-03: Legal, regulatory, and contractual requirements regarding cybersecurity — including privacy and civil liberties obligations — are understood and managed.	3	Subcategory/Security Controls are covered in Mission Objective 3	
	GV.RM-03: Cybersecurity risk management activities and outcomes are included in enterprise risk management processes.	3	Subcategory/Security Controls are covered in Mission Objective 3	
	GV.RR-02: Roles, responsibilities, and authorities related to cybersecurity risk management are established,	3	PM-02: Information Security Program Leadership Role PM-13: Security and Privacy Workforce	PM-13 was not chosen because workforce management for security and privacy is low priority due to automated CCTV

Objective	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
	communicated, understood, and enforced.		PM-19: Privacy Program Leadership Role PM-23: Data Governance Body PM-24: Data Integrity Board PM-29: Risk Management Program Leadership Roles	operations with limited 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 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	

Objective	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
	GV.PO-02: Policy for managing cybersecurity risks is reviewed, updated, communicated, and enforced to reflect changes in requirements, threats, technology, and organizational mission.	3	Same controls as GV.PO-01	
	GV.SC-02: Cybersecurity roles and responsibilities for suppliers, customers, and partners are established, communicated, and coordinated internally and externally.	3	SR-02: Supply Chain Risk Management Plan SR-03: Supply Chain Controls and Processes SR-05: Acquisition Strategies, Tools, and Methods	
	ID.AM-04: Inventories of services provided by suppliers are maintained.	3	AC-20: Use of External Systems SA-09: External System Services SR-02: Supply Chain Risk Management Plan	
	ID.AM-07: Inventories of data and corresponding metadata for designated data types are maintained.	3	Subcategory/Security Controls are covered in Mission Objective 3	
	ID.AM-08: Systems, hardware, software, services, and data are managed throughout their lifecycles.	3	Subcategory/Security Controls are covered in Mission Objective 1	
	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	3	Subcategory/Security Controls are covered in Mission Objective 1	

Objective	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
	vulnerabilities are identified and recorded.			
	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		
	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	3	Subcategory/Security Controls are covered in Mission Objective 3	

Objective	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
	perform general tasks with cybersecurity risks in mind.			
	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 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	

Objective	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
			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	CM-10 was not chosen because CCTV systems primarily use embedded firmware with limited user interaction, rendering software licensing and peer-to-peer file sharing restrictions less applicable.
	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	

Objective	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
	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 #11: Enhance Telecommunications and Networking to Facilitate Emerging ITS Capabilities	GV.RM-07: Strategic opportunities (i.e., positive risks) are characterized and are included in organizational cybersecurity risk discussions.	3	Subcategory/Security Controls are covered in Mission Objective 1	
	GV.RR-02: Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced.	3	Subcategory/Security Controls are covered in Mission Objective 8	
	GV.OV-01: Cybersecurity risk management strategy outcomes are reviewed to inform and adjust strategy and direction.	3	Subcategory/Security Controls are covered in Mission Objective 1	
	GV.OV-02: The cybersecurity risk management strategy is reviewed and adjusted to ensure coverage of organizational requirements and risks.	3	PM-09: Risk Management Strategy PM-18: Privacy Program Plan PM-30: Supply Chain Risk Management Strategy	

Objective	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
			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.OV-03: Organizational cybersecurity risk management performance is evaluated and reviewed for adjustments needed.	3	AC-01 Policy and Procedures AT-01 Policy and Procedures AU-01 Policy and Procedures CA-01 Policy and Procedures CM-01 Policy and Procedures CP-01: Policy and Procedures IA-01: Policy and Procedures IR-01: Policy and Procedures MA-01: Policy and Procedures MP-01: Policy and Procedures PE-01: Policy and Procedures PL-01: Policy and Procedures PM-01: Information Security Program Plan PS-01: Policy and Procedures PT-01: Policy and Procedures RA-01: Policy and Procedures SA-01: Policy and Procedures SC-01: Policy and Procedures SI-01: Policy and Procedures	

Objective	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
			SR-01: Policy and Procedures PM-28: Risk Framing	
	GV.SC-02: Cybersecurity roles and responsibilities for suppliers, customers, and partners are established, communicated, and coordinated internally and externally.	3	Subcategory/Security Controls are covered in Mission Objective 8	
	ID.AM-01: Inventories of hardware managed by the organization are maintained.	3	Subcategory/Security Controls are covered in Mission Objective 1	
	ID.AM-02: Inventories of software, services, and systems managed by the organization are maintained.	3	Subcategory/Security Controls are covered in Mission Objective 1	
	ID.AM-03: Representations of the organization's authorized network communication and internal and external network data flows are maintained.	3	Subcategory/Security Controls are covered in Mission Objective 3	
	ID.AM-04: Inventories of services provided by suppliers are maintained.	3	Subcategory/Security Controls are covered in Mission Objective 8	
	ID.AM-05: Assets are prioritized based on classification, criticality, resources, and impact on the mission.	3	RA-03: Risk Assessment RA-09: Criticality Analysis RA-02: Security Categorization	
	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	CA-07: Continuous Monitoring CM-03: Configuration Change Control CM-04: Impact Analyses	
	ID.IM-01: Improvements are identified from evaluations.	3	Subcategory/Security Controls are covered in Mission Objective 1	
	ID.IM-04: Incident response plans and other cybersecurity plans that affect operations are established, communicated, maintained, and improved.	3	Subcategory/Security Controls are covered in Mission Objective 1	
	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	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-6 was not chosen because establishing and enforcing configuration settings is covered by higher-priority technical controls, with CCTV relying on manufacturer defaults and network baselines.

Objective	Subcategory	Affinity Score	NIST SP 800-53 Mapped Controls	Notes
			CM-08: System Component Inventory CM-09: Configuration Management Plan CM-10: Software Usage Restrictions CM-11: User-Installed Software	
	PR.PS-04: Log records are generated and made available for continuous monitoring.	3	Subcategory/Security Controls are covered in Mission Objective 3	
	PR.IR-01: Networks and environments are protected from unauthorized logical access and usage.	3	Subcategory/Security Controls are covered in Mission Objective 3	
	PR.IR-03: Mechanisms are implemented to achieve resilience requirements in normal and adverse situations.	3	Subcategory/Security Controls are covered in Mission Objective 1	
	DE.CM-01: Networks and network services are monitored to find potentially adverse events.	3	Subcategory/Security Controls are covered in Mission Objective 1	

Appendix C. Abbreviations

ARC-IT	Architecture Reference for Cooperative and Intelligent Transportation
ATT&CK	Adversarial Tactics, Techniques, and Common Knowledge
CCTV	closed-circuit television
CIS	Center for Internet Security
CSF	Cybersecurity Framework
CVO	Commercial Vehicle Operations
DAS	direct attached storage
DM	Data Management
DoS	denial of service
DVR	digital video recorder
EMP	electromagnetic pulse
FIPS	Federal Information Processing Standard
FTP	File Transfer Protocol
G	guidance
HTTPS	Hypertext Transfer Protocol Secure
ICS	industrial control system
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IOO	infrastructure owner/operator
IP	internet protocol
IPSec	Internet Protocol Security
ITS	Intelligent Transportation System
LAN	local area network
L-M-H	low, moderate, and high
M	manufacturer
M/I	manufacturer/IOO
MC	Maintenance and Construction
NAS	network attached storage
NIST	National Institute of Standards and Technology
NS	not selected
NTCIP	National Transportation Communications for Intelligent Transportation System Protocol

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

NVR	network video recorder
OT	operational technology
PII	personally identifiable information
PLC	programmable logic controller
PM	Parking Management
PS	Public Safety
PT	Public Transportation
PV	parameter value
R	risk
RFC	request for comment
RSA	Rivest–Shamir–Adleman
S	standard
SAN	storage area network
SCADA	Supervisory Control and Data Acquisition
SP	Special Publication
SSH	secure shell
ST	Sustainable Travel
TCP	Transmission Control Protocol
TI	Traveler Information and Personal Mobility
TLS	Transport Layer Security
TM	Traffic Management
TMC	traffic management center
UDP	User Datagram Protocol
V	value
VLAN	virtual local area network
VMS	video management system
VPN	virtual private network
VS	Vehicle Safety
WAN	wide area network
Wi-Fi	wireless fidelity
WLAN	wireless LAN
WX	Weather

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

Control Extension	A statement that extends the basic capability of a control by specifying additional functionality, altering the strength mechanism, or adding or limiting implementation options.
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. Note: 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 confidentiality, integrity, and availability, 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 TMC manager is a component of State government). Enterprise objects may participate wholly or in part in other enterprise objects (e.g., a device developer is a component of auto manufacturer but also participates in standards body).
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 to 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 encompasses a broad range of wireless and wireline communications-based information and electronics technologies.
Closed-circuit Television	A distribution system which limits reception of an image to those receivers or monitors which are directly connected to the origination point by coaxial cable or microwave link.
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 make up the ITS and the surrounding environment. They are defined in terms of the services they support, the processing they include, and their interfaces with other physical objects. They are grouped into six classes: centers, field, ITS, support, travelers, and vehicles. Example physical objects are the TMC, the vehicle onboard equipment, and the ITS roadway equipment. These correspond to the physical world: respectively traffic operations centers, equipped connected automobiles, and roadside signal controllers. Due to this close correspondence between the physical world and the physical objects, the interfaces between them are prime candidates for standardization. In ARC-IT, physical objects are defined with scope such that they are under the control of a single enterprise object.

Risk Tolerance

The organizations or stakeholder's readiness to bear the risk after risk of treatment to achieve its objectives. Risk tolerance can be influenced by legal or regulatory requirements.

Roadside Unit

A fixed-position cooperative device. This may be a permanent installation or temporary equipment brought on-site for a period associated with an incident, road construction, or other event.

Service Package

Provides an accessible, service-oriented perspective to ARC-IT and are tailored to fit, separately or in combination, real world transportation problems, and needs. Service packages collect one or more functional objects that must work together to deliver a given ITS service, and the information flows that connect them and other important external systems. In other words, they identify the pieces of the physical view that are required to implement a particular ITS service. Service packages are implemented through projects (or groups of projects, aka programs) and in transportation planning, are related to ITS strategies used to meet regional goals and objectives.

References

1. The National ITS Reference Architecture. n.d. "TM01: Infrastructure-Based Traffic Surveillance." Washington, DC. U.S. Department of Transportation. <https://www.arc-it.net/html/architecture/architecture.html>, last accessed October 9, 2025.
2. 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.
3. 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.
4. 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 10, 2025.
5. 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.
6. 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.
7. 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.
8. 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.
9. ARC-IT Version 9.3. n.d. "Service Packages." The National ITS Reference Architecture. <https://www.arc-it.net/html/servicepackages/servicepackages-areaspport.html>, last accessed October 10, 2025.
10. 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.
11. 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.
12. 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.

13. ARC-IT Version 9.3. n.d. "Notes on Access Control." <https://www.arc-it.net/html/security/controlsclarification.html>, last accessed October 14, 2025.
14. 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.
15. National Transportation Communications for ITS Protocol. 2021. *Infrastructure Standards Security Assessment (ISSA)*. NTCIP 9014 v01.20. Published August 2021. American Association of State Highway and Transportation Officials (AASHTO), Institute of Transportation Engineers (ITE), and National Electrical Manufacturers Association (NEMA). <https://www.ntcip.org/file/2021/08/NTCIP9014v0120.pdf>, last accessed October 15, 2025.
16. National Institute of Standards and Technology. 2001. *Security Requirements for Cryptographic Modules*. Federal Information Processing Standard Publication FIPS PUB 140-2 (superseded). Issued May 25, 2001. Washington, DC. U.S. Department of Commerce. <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf>, last accessed October 10, 2025.
17. National Institute of Standards and Technology. 2022. *Personal Identity Verification (PIV) of Federal Employees and Contractors*. Federal Information Processing Standard Publication. FIPS PUB 201-3. Issued January 2022. Washington, DC. U.S. Department of Commerce. <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-3.pdf>, last accessed October 10, 2025.
18. National Institute of Standards and Technology. 2019. *Security Requirements for Cryptographic Modules*. Federal Information Processing Standard Publication FIPS PUB 140-3. Issued March 22, 2019. Washington, DC. U.S. Department of Commerce. <https://csrc.nist.gov/publications/detail/fips/140/3/final>, last accessed October 10, 2025.
19. 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.
20. Cybersecurity & Infrastructure Security Agency. n.d. "Cybersecurity Alerts & Advisories" (web page). <https://www.cisa.gov/news-events/cybersecurity-advisories>, last accessed October 10, 2025.
21. National Institute of Standards and Technology. n.d. National Vulnerability Database. <https://nvd.nist.gov/>, last accessed October 10, 2025.
22. 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. <https://csrc.nist.gov/pubs/sp/800/90/a/r1/final>, last accessed October 15, 2025.
23. Internet Engineering Task Force (IETF). 2008. *The Transport Layer Security (TLS) Protocol Version 1.2*. Request for Comment 8446. RCF Editor. August 2008. <https://www.ietf.org/rfc/rfc5246.txt>, last accessed October 15, 2025.
24. National Institute of Standards and Technology. *Advanced Encryption Standard (AES)*. Federal Information Processing Standards Publication. FIPS 197. Published November 26, 2001; updated May 9, 2023. Washington, DC. U.S. Department of Commerce. <https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.197.pdf>, last accessed October 14, 2025.

25. National Institute of Standards and Technology. 2011. *BIOS Protection Guidelines*. NIST SP 800-147. April 2011. Washington, DC. U.S. Department of Commerce. <https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-147.pdf>, last accessed October 14, 2025.
26. International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC). 2022. Information security, cybersecurity and privacy protection — Information security controls. management systems — Requirements. ISO/IEC 27001:2022, published February 2022. <https://www.iso.org/standard/82423.html>, last accessed November 4, 2025. <https://www.iso.org/standard/27001>, last accessed November 4, 2025
27. 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
28. 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.
29. National Transportation Communications for ITS Protocol. 2001. *National Transportation Communications for ITS Protocol Object Definitions for Closed Circuit Television (CCTV) Camera Control*. NTCIP 1205 v01.08. Published December 2001. American Association of State Highway and Transportation Officials (AASHTO), Institute of Transportation Engineers (ITE), and National Electrical Manufacturers Association (NEMA). <https://www.ntcip.org/wp-content/uploads/2018/11/NTCIP1205v0108b.pdf>, last accessed November 4, 2025.
30. National Institute of Standards and Technology. 2016. *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security*. NIST SP 800-46 Rev 2. Published July 2016. Washington, DC. U.S. Department of Commerce. <https://csrc.nist.gov/pubs/sp/800/46/r2/final>, last accessed November 4, 2025.
31. 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.
32. 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.
33. 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.
34. National Institute of Standards and Technology. 2007 *Guide to Intrusion Detection and Prevention Systems (IDPS)*. NIST SP 800-94. Published February 2007. Washington, DC. U.S. Department of Commerce. <https://csrc.nist.gov/pubs/sp/800/111/final>, last accessed November 4, 2025.

35. National Institute of Standards and Technology. 2011. *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*. NIST SP 800-137. Published September 2011. Washington, DC. U.S. Department of Commerce. <https://csrc.nist.gov/pubs/sp/800/137/final>, last accessed November 4, 2025.
36. National Institute of Standards and Technology. 2010. *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*. NIST SP 800-122. Published April 2010. Washington, DC. U.S. Department of Commerce. <https://csrc.nist.gov/pubs/sp/800/122/final>, last accessed November 4, 2025.
37. 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.
38. 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
39. 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.
40. 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.
41. 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.
42. 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.
43. 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.
44. 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

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-26-002



U.S. Department of Transportation